Upgrading the Policy Controller

What's new in SN08

The Policy Controller is a new component in the CS 2000 network of components.

General upgrade strategy for SN08

The Policy Controller is a new component in the CS 2000 network of components. Therefore, there are no software upgrades from releases previous to SN08. The current release of the NCGL platform software can be patched or upgraded by way of a maintenance release upgrade, while the current release of the Policy Controller application software can be upgraded only by way of a maintenance release upgrade.

Activities and procedures are available in this NTP for performing both patching and maintenance release upgrade activities as well as activities for aborting an upgrade. Release notes provided with the patch files or maintenance release images offer additional information about performing these activities.

Document References

You need the following documents for this upgrade procedure.

Document name	Document number
Policy Controller Security and Administration	NN10434-611
Policy Controller Configuration Management	NN10432-511
Policy Controller Fault Management	NN10438-911
Upgrading the Policy Controller	NN10431-461

Tools and utilities for maintenance releases

You upgrade the Policy Controller by using different interfaces depending on the procedure required. The interface required is described at the beginning of each procedure. Use the following

interfaces to perform the procedures in this NTP and are accessed through network workstations or the Integrated Element Management System (IEMS):

- The Policy Controller Manager GUI, a client web browser application, launched from the IEMS client.
- The CS 2000 NCGL Platform Manager GUI, a client web browser application, launched from the IEMS client.
- The NCGL command line interface (CLI).

Interfaces used to apply maintenance releases

The following interfaces are used in applying maintenance releases:

- The Policy Controller Manager GUI, a client web browser application, launched from the IEMS client.
- The CS 2000 NCGL Platform Manager GUI, a client web browser application, launched from the IEMS client.
- The NCGL command line interface (CLI)

Interfaces used to apply patches to the NCGL platform

The NCGL Platform Patching is performed manually using the NCGL command line interface (CLI) available on each NCGL node to be patched.

Applying a maintenance release upgrade

This section describes how to perform:

- an in-service maintenance release (MR) upgrade of the Policy Controller units
- a rollback of a partial or complete MR upgrade in cases where a maintenance release fails or causes problems with the system.

Maintenance release upgrade strategy

There are two types of Maintenance releases for the Policy Controller: An MR type for the NCGL platform and another MR type for the Policy Controller application.

- **An NCGL platform MR** consists of release notes, CS 2000 NCGL Platform Manager software, NCGL software and optional CS 2000 NCGL Platform Manager patches.

  Using the CS 2000 NCGL Platform Manager GUI you can select an MR image to upgrade from. You can upgrade the Policy Controller load from the local DVD-ROM drive, from an ISO image located on a remote system, or from a local file on the Policy Controller disk drive. Space is available on the local hard drive to maintain

approximately 2 loads in case fallback to a previous load is necessary. Partial and complete rollbacks of a failed upgrade can be performed.

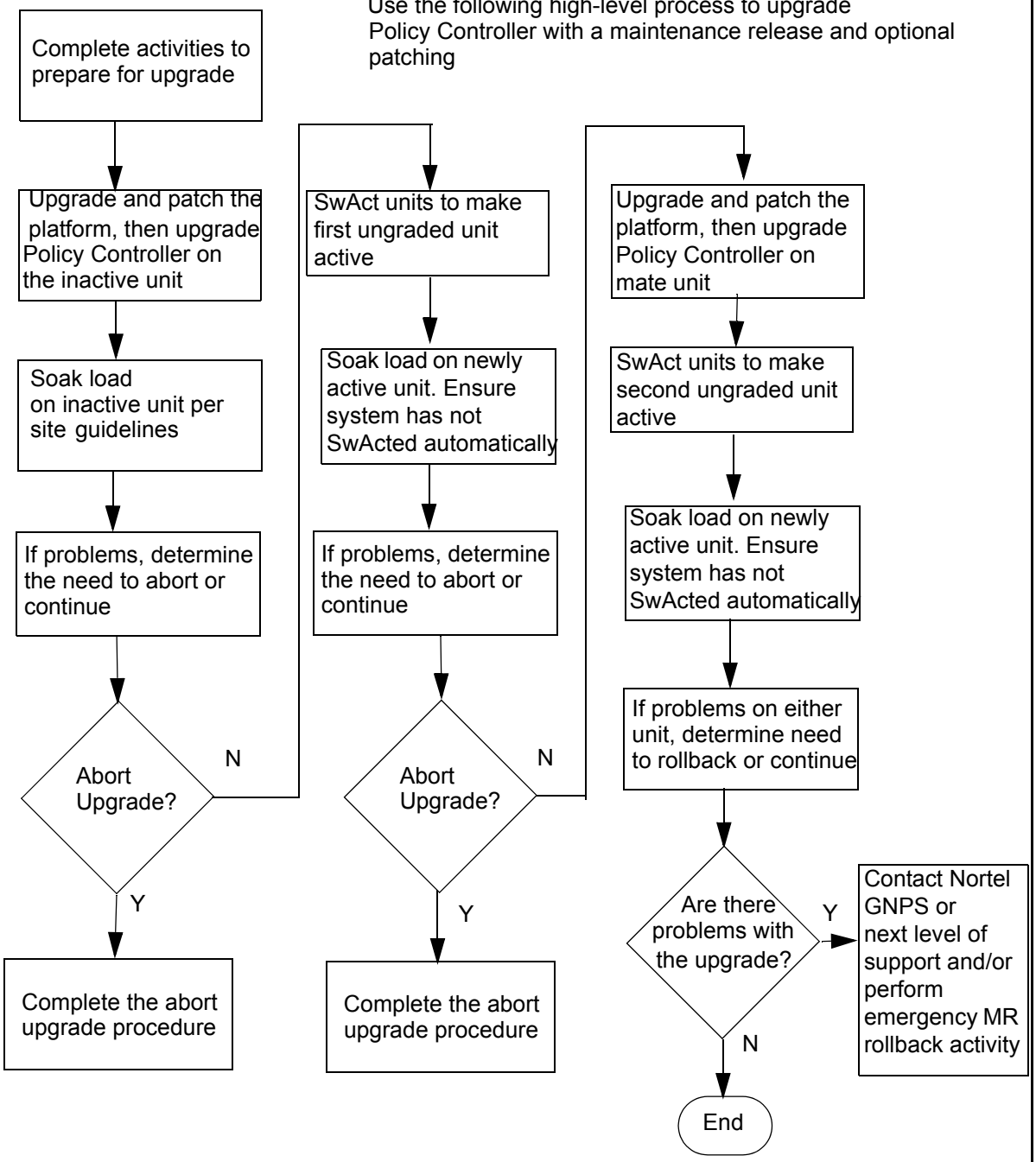
- **A Policy Controller MR** consists of release notes, CS 2000 NCGL Platform Manager software, Policy Controller application software and optional CS 2000 NCGL Platform Manager patches.

  Using both the CS 2000 NCGL Platform Manager GUI and the Policy Controller command line interface (CLI), you can upgrade the Policy Controller application.

Refer to the following diagram for a high-level view of the upgrade process for the Policy Controller units.

Upgrading the Policy Controller with an MR

Use the following high-level process to upgrade Policy Controller with a maintenance release and optional patching



Maintenance release limitations and restrictions

The following general limitations apply to performing a maintenance release upgrade or rollback of an MR upgrade.

- While an MR upgrade is an in-service upgrade, performing an emergency rollback of a maintenance release is an out-of-service activity. During an out-of-service upgrade, the Policy Controller will stop functioning as a Network Virtual Call Admissions Control (NVCAC) device. All Network VCAC processes will be affected and calls on the CS 2000 will continue without the Virtual Call Admission Control function.
- Only NCGL Platform patching is supported in SN08 maintenance releases. Policy Controller application patches are not supported in SN08.
- Patches can only be applied using the CLI (command line interface).
- If there have been changes to the Policy Controller database since you last backed it up, do not use the backup copy that contains the old database to restore it. The result can be file corruption, partially imported data, or a complete failure of the restore.

Software delivery methods for maintenance releases

MR software is delivered on a data DVD-ROM or using Electronic Software Delivery (ESD,) where a compressed ISO image is delivered to an electronic drop-box on the customer network from Nortel Networks.

MR upgrades using ESD delivery require that the MR package be transferred onto both Policy Controller units and put in the /opt/swd directory using a secure file transfer program such as scp. After the MR upgrade of the NCGL platform the bootload file is stored in the /boot directory.

In order to receive maintenance releases from Nortel using ESD the operating company must have an ESD agreement with Nortel. When the agreement is established, the operating company provides Nortel with the location of an electronic dropbox, an E-mail address for notification and a username and password pair for delivering software loads. When Nortel delivers a software load to the dropbox, an electronic mail notification is sent to the E-mail address specified by the operating company.

Software installation methods for maintenance releases

You can upgrade the Policy Controller NCGL load from the local DVD-ROM drive, or from an ISO image located on a remote system, or

copied to a local directory. The following upgrade protocols (methods) are selectable from the Policy Controller Manager GUI:

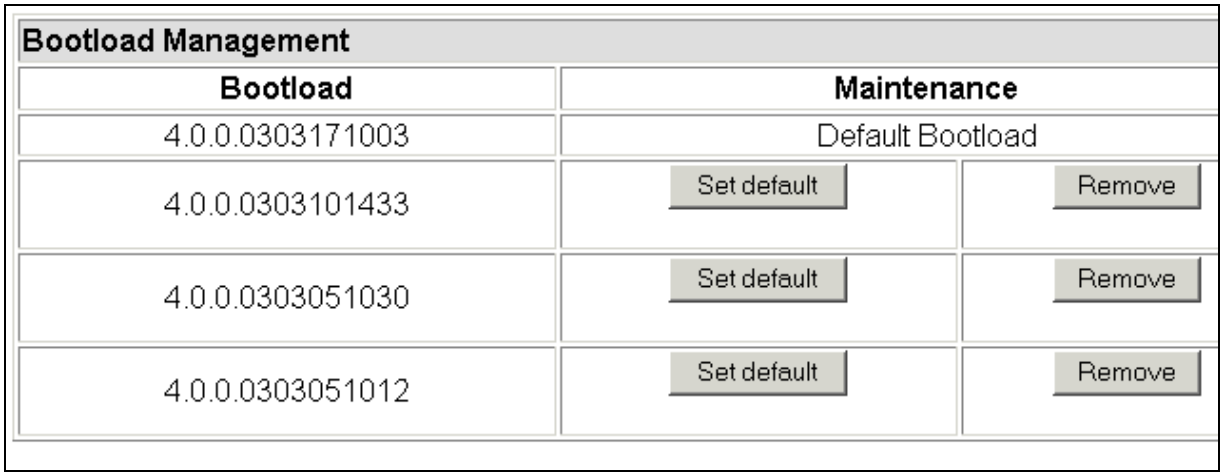
- Local CDROM - the local DVD-ROM drive (labelled as the local CD-ROM).
- Local file - an iso image, or load.tgz file copied from the local DVD-ROM drive copied to the hard drive using the secure copy program, **scp**, to transfer the data.
- Remote file using FTP or anonymous FTP - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP service. If the workstation or server is configured to allow anonymous FTP, use anonymous FTP to avoid sending username and password information in clear text format across the network. This is not a recommended method.
- Remote file using HTTP or HTTPS - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP or HTTPS service. This is not a recommended method.

You can upgrade the Policy Controller application from the local DVD-ROM drive, or from an ISO image copied to a local directory. Most of the time the MR for the Policy Controller application is on the same DVD-ROM disk or copied ISO image as the NCGL platform load; however, some customers may receive a separate maintenance release load that contains an MR only for the Policy Controller application. Consult your release notes for details.

Removing older NCGL bootload versions

By default, the Policy Controller units retain previous bootloads. Older bootload versions may be manually removed by clicking the **Remove** button using the Web GUI (see graphic below). You cannot delete the bootload that is set to be the default bootload, nor can you delete the currently running bootload.

If a bootload image upgrade is requested and insufficient disk space is available in the `/boot` directory, the NCGL software deletes the oldest bootload from the `/boot` directory and performs the requested bootload image upgrade. The system can not delete a bootload that is set to be the default bootload.



Bootload Management		
Bootload	**Maintenance**	
4.0.0.0303171003	Default Bootload	
4.0.0.0303101433	Set default	Remove
4.0.0.0303051030	Set default	Remove
4.0.0.0303051012	Set default	Remove

Upgrade preparation

Complete the steps in the Upgrade preparation table below.

Upgrade preparation

Step	Procedure
1	If you have purchased security certificates from a Certificate Authority, then ensure that you have made a backup copy of the following security certificate files: server.key, server.crt and certificate.keystore. These files are located in directory /opt/base/share/ssl. Otherwise, transfer a copy of the default security certificate files (same names and location as above) to a secure location on a remote server. For more information on security certificates for Policy Controller refer to the Security and Administration NTP, NN10434-611.
2	Backup the Policy Controller application database on the active unit using procedure Perform a manual backup of the Policy Controller database on page 149.
3	Acquire the appropriate maintenance release software from Nortel either using ESD delivery to a customer dropbox/repository server or from a maintenance release DVD-ROM disk.
4	If performing a maintenance release upgrade with an ISO image acquired using ESD, complete procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 31 to copy ISO files to hard drive of each unit.

Upgrade preparation

Step	Procedure
5	Use procedure View release notes for a maintenance release on page 35 to check release notes for the applicability of the MR.
6	Locate and have available the original Policy Controller software DVD-ROM along with a copy of the existing version of the Policy Controller application installed on your system. The existing version may be from the last maintenance release image installed from a DVD-ROM or an ESD downloaded image file.
7	Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
8	You have completed this high-level procedure.

Perform a maintenance release upgrade

Complete the following steps, in the order listed, to perform an in-service maintenance release upgrade and optional patching of the NCGL platform and to perform a maintenance release upgrade of the Policy Controller application.

Maintenance release upgrade

Step	Procedure
Upgrade the NCGL platform load on first unit	
9	Complete Section Upgrade preparation on page 7.
10	Determine what version of the NCGL platform load is currently installed on your Policy Controller node by going to the ***System Info*** page of the CS 2000 NCGL Platform manager and using procedure View the operational status of a Policy Controller NCGL platform on page 43. Determine what version of the Policy Controller application software (listed as Policy Controller load info) is currently installed on your Policy Controller node using procedure Determine the current version of software loads on page 64.

Maintenance release upgrade

Step	Procedure
11	Compare the current version of the NCGL Platform Load installed with the MR release notes to determine if you must upgrade the NCGL platform load with a newer maintenance release. Also use to determine if you need to upgrade to a previously released MR first. If the MR contains a newer version of the NCGL platform load than what is currently installed, then proceed with this upgrade. If not then you do not need a maintenance release upgrade. Skip to step 17 to determine if there are any NCGL patches that need to be applied and committed on the inactive unit.
12	If applying an MR upgrade using a DVD-ROM, insert the disk into the disk drive of the inactive unit.
13	Log onto the active unit and use procedure Prevent a system SwAct (Jam) on page 39 to jam the units.
14	Log onto the inactive unit and upgrade the NCGL platform software using procedure Upgrade Policy Controller NCGL platform software on page 66.
15	Log into the active Policy Controller unit, use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure Reboot a Policy Controller unit on page 73 for assistance.
16	After the inactive unit completes rebooting, log into the inactive unit, use the CS 2000 NCGL Platform Manager and go to the **System Info** page to verify that the Current version of the NCGL software matches the expected new version. Use procedure View the operational status of a Policy Controller NCGL platform on page 43 for assistance with this task.
Apply and commit NCGL patches to the first unit	
17	Use procedure Patching the NCGL platform on page 24 to apply and commit NCGL patches to the inactive unit.

Maintenance release upgrade

Step	Procedure
Upgrade the Policy Controller application software on the first unit	
18	On the inactive unit, upgrade the Policy Controller application software using procedure Upgrade/rollback/reinstall the Policy Controller application on page 93.
19	Log into the inactive unit's CLI and verify that the current version of the Policy Controller application matches the expected new version by executing the following command: $ **cat /opt/apps/webint/version_info.txt.**
Activate and soak the new load on the first unit	
20	From the active unit, verify that the Policy Controller application databases on both units have synchronized using procedure Verify synchronization status of Policy Controller units on page 99
21	Use procedure Enable a system SwAct (Unjam) on page 107 to unjam the units.
22	As applicable to your site, test new software on the inactive unit. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing Only go forward to SwAct when all the tests have passed.
23	From the active unit perform a SwAct of the units using procedure Invoke a maintenance SwAct of the Policy Controller platform on page 103.

Maintenance release upgrade

Step	Procedure
24	As applicable to your site, test new software on upgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing. **CAUTION**: Perform a check to ensure the system has not SwActed automatically after the software upgrade. An automatic system SwAct could be initiated if a fault is detected by the system. This will be indicated in the alarms and logs. However, it is still advisable to use the procedure View the operational status of a Policy Controller NCGL platform on page 43 to confirm the active units software load is as expected before proceeding to upgrade the second Policy Controller unit.
25	If all software tests are successful, continue with the next step in this procedure to upgrade the second (mate) Policy Controller unit (now inactive). Otherwise, if the active unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure and complete procedure Abort a maintenance release upgrade on page 16 and contact your next level of support or Nortel GNTS.
Upgrade the NCGL platform load on second unit	
26	Verify that all applicable activities in Section Upgrade preparation on page 7 have been completed for the second unit.

Maintenance release upgrade

Step	Procedure
27	Determine what version of the NCGL platform load is currently installed on the second unit using procedure by going to the **System Info** page of the CS 2000 NCGL Platform manager, using procedure View the operational status of a Policy Controller NCGL platform on page 43. Determine what version of the Policy Controller application software (listed as Policy Controller load info) is currently installed on the second unit using procedure Determine the current version of software loads on page 64.
28	Compare the current version of the NCGL Platform Load installed with the MR release notes to determine if you must upgrade the NCGL platform load on the second unit with a newer maintenance release. If the MR contains a newer version of the NCGL platform load than what is currently installed, then proceed with this upgrade. If not then you do not need to apply a maintenance release upgrade, skip to step 31 to perform any necessary patching of this unit.
29	If applying an MR upgrade using a DVD-ROM, insert the disk into the disk drive of the inactive unit.
30	Log onto the active unit and use procedure Prevent a system SwAct (Jam) on page 39 to verify that the units are still jammed. If they are not, then jam the units.
31	Log onto the inactive unit and upgrade the NCGL platform software using procedure Upgrade Policy Controller NCGL platform software on page 66.
32	Log into the active Policy Controller unit, use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure Reboot a Policy Controller unit on page 73 for assistance.

Maintenance release upgrade

Step	Procedure
33	After the inactive unit completes rebooting, log into the inactive unit, use the CS 2000 NCGL Platform Manager and go to the **System Info** page to verify that the Current version of the NCGL software matches the expected new version. Use procedure View the operational status of a Policy Controller NCGL platform on page 43 for assistance with this task.
Apply and commit NCGL patches to the second unit	
34	Use procedure Patching the NCGL platform on page 24 to apply and commit NCGL patches to the inactive unit.
Upgrade the Policy Controller application software on the second unit	
35	On the inactive unit, upgrade the Policy Controller application software using procedure Upgrade/rollback/reinstall the Policy Controller application on page 93.
36	Log into the inactive unit's CLI and verify that the current version of the Policy Controller application matches the expected new version by executing the following command: $ **cat /opt/apps/webint/version_info.txt.**
Activate and soak the new load on the second unit	
37	From the active unit, verify that the Policy Controller application databases on both units have synchronized using procedure Verify synchronization status of Policy Controller units on page 99
38	Use procedure Enable a system SwAct (Unjam) on page 107 to unjam the units.

Maintenance release upgrade

Step	Procedure
39	As applicable to your site, test new software on the inactive unit. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing Only go forward to SwAct when all the tests have passed.
40	From the active unit perform a SwAct of the units using procedure Invoke a maintenance SwAct of the Policy Controller platform on page 103.
41	As applicable to your site, test new software on the upgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing. **CAUTION**: Perform a check to ensure the system has not SwActed automatically after the software upgrade. An automatic system SwAct could be initiated if a fault is detected by the system. This will be indicated in the alarms and logs. However, it is still advisable to use the procedure View the operational status of a Policy Controller NCGL platform on page 43 to confirm the active units software load is as expected before proceeding to upgrade the second Policy Controller unit.

Maintenance release upgrade

Step	Procedure
42	If all software tests are successful, continue with the next step in this procedure. Otherwise, if the active unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure. Go to and complete the steps in procedure Perform an emergency maintenance release rollback on page 19 and contact your next level of support, Nortel GNPS, or Nortel's emergency response.
43	From the active unit, verify that the Policy Controller application databases on both units have synchronized using procedure Verify synchronization status of Policy Controller units on page 99
44	Monitor the system for an appropriate period per your site guidelines before declaring this maintenance release complete.
45	Refer to procedure *Editing or viewing properties of objects* in the Integrated EMS Configuration Management NTP, NN10330-511. Locate the Policy Controller element associated with the node you upgraded and select the correct major version number for the Device Version field
46	You have completed the maintenance release upgrade procedure.

Abort a maintenance release upgrade

ATTENTION
This procedure assumes that you have not upgraded the second Policy Controller unit in the node with the maintenance release. If you have already upgraded both units with the maintenance release, then contact your next level of support or Nortel GNPS.

Complete the following steps, in the order indicated, to abort a maintenance release upgrade procedure in progress.

Abort maintenance release

Step	Procedure
47	If necessary, use procedure Enable a system SwAct (Unjam) on page 107 to unjam the units.
48	If necessary, complete procedure Invoke a maintenance SwAct of the Policy Controller platform on page 103 to revert call processing to the un-upgraded unit (the unit that is operating with the pre-maintenance release load).
49	Use procedure Prevent a system SwAct (Jam) on page 39 to verify that the units are jammed. If they are not, then jam the units.
50	Log onto the inactive unit and use procedure Rollback a Policy Controller NCGL platform software upgrade on page 111 to set the default NCGL bootfile to the pre-MR load (the load the unit operated on prior to the maintenance release upgrade).
51	Log into the active Policy Controller unit, use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a FORCED reboot (RebootMate) of the inactive (mate) unit. Refer to procedure Reboot a Policy Controller unit on page 73 for assistance. ***Note:*** All committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying patches is not required.

Abort maintenance release

Step	Procedure
52	On the inactive unit CLI use the pre-MR DVD-ROM or pre-MR Policy Controller application ISO image to downgrade the Policy Controller application software using procedure Upgrade/rollback/reinstall the Policy Controller application on page 93.
53	From the active unit, verify that the Policy Controller application databases on both units have synchronized using procedure Verify synchronization status of Policy Controller units on page 99.
54	Once the databases are in sync, release the JAM on the units using procedure Enable a system SwAct (Unjam) on page 107.
55	Complete procedure Invoke a maintenance SwAct of the Policy Controller platform on page 103 to make the downgraded unit active.
56	As applicable to your site, test the software on the downgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.

Abort maintenance release

Step	Procedure
57	Monitor the system for an appropriate period per your site guidelines before declaring this maintenance release complete. If all software tests are successful, continue with the next step. Otherwise, if the active unit (with downgraded load) experiences problems with call processing, perform the following tasks in order: • complete procedure Invoke a maintenance SwAct of the Policy Controller platform on page 103 • complete procedure Prevent a system SwAct (Jam) on page 39 • contact your next level of support or Nortel GNPS.
58	You have completed this high-level abort procedure.

Perform an emergency maintenance release rollback

CAUTION

This procedure is a service affecting. Performing an emergency maintenance release rollback causes approximately a one hour service interruption.

Complete the following steps, in the order indicated, to roll back a maintenance release upgrade that has been performed on both Policy Controller units in the node.

Emergency maintenance release rollback

Step	Procedure
59	Locate and have available the previous Policy Controller software DVD-ROM or an ESD downloaded image file of the previous maintenance release. Ensure that you have available a recent backup copy of the Policy Controller application database, for the downgraded software version. ***Note:*** There is a potential for database corruption if the database backup is from a different software load to the load being restored.
60	If performing a maintenance release rollback using an ISO image acquired using ESD, verify that the applicable ISO files are copied to the hard drive of each unit. If necessary, use procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 31.
61	Log onto the active unit CLI and complete procedure Drop database synchronization for the Policy Controller application on page 115 executed from the current release of the Policy Controller software DVD-ROM or from the currently installed ISO image. ***Note:*** Once executed, this script drops call processing and application database synchronization between the active and inactive units. The Policy Controller application maintains this non-synchronized state until a manual SwAct is performed, later in the procedure.

Emergency maintenance release rollback

Step	Procedure
62	Log onto the inactive unit and use procedure Rollback a Policy Controller NCGL platform software upgrade on page 111 to set the default NCGL bootfile to the pre-MR load (the load the unit operated on prior to the maintenance release upgrade). ***Note:*** All committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying patches is not required.
63	Using the CS 2000 NCGL Platform Manager, go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure Reboot a Policy Controller unit on page 73 for assistance.
64	On the inactive unit, rollback the Policy Controller application software. Complete procedures Upgrade/rollback/reinstall the Policy Controller application on page 93.
65	On the inactive unit, prepare to restore a backup copy of the Policy Controller application database using procedure Prepare for a database restore on a Policy Controller unit on page 139.
66	On the inactive unit (the rolled back unit), install the backup copy of the Policy Controller application database using procedure Perform a database restore to a Policy Controller unit on page 153.
67	Perform a SwAct (Force) of the units by completing procedure Invoke a maintenance SwAct of the Policy Controller platform on page 103 to make the downgraded unit active.

Emergency maintenance release rollback

Step	Procedure
68	As applicable to your site, test the software on the downgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* and to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
69	Monitor the system for an appropriate period per your site guidelines before declaring this rollback complete. If all software tests are successful, continue with the next step. Otherwise, if the active unit (with rolled back load) experiences problems with call processing, STOP executing the procedure and contact your next level of support or Nortel GNPS.
70	Use procedure Prevent a system SwAct (Jam) on page 39 to jam the units.
71	Log onto the inactive unit and use procedure Rollback a Policy Controller NCGL platform software upgrade on page 111 to set the default NCGL bootfile to the pre-MR load (the load the unit operated on prior to the maintenance release upgrade). ***Note:*** All committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying patches is not required.
72	Use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure Reboot a Policy Controller unit on page 73 for assistance.

Emergency maintenance release rollback

Step	Procedure
73	On the inactive unit, rollback the Policy Controller application software using procedure Upgrade/rollback/reinstall the Policy Controller application on page 93.
74	From the active unit, verify that the Policy Controller application databases are synchronizing using procedure Verify synchronization status of Policy Controller units on page 99. If they are synchronizing then go to step 76. If they are not synchronizing then go to the next step.
75	Use procedure View the operational status of a Policy Controller NCGL platform on page 43 to check the status of the inactive unit to determine why database synchronization is not taking place by reviewing existing faults and logs. Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
76	Once the databases are in sync, release the JAM on the units using procedure Enable a system SwAct (Unjam) on page 107.
77	Perform a SwAct of the units by completing procedure Invoke a maintenance SwAct of the Policy Controller platform on page 103 to make the downgraded unit active.

Emergency maintenance release rollback

Step	Procedure
78	Monitor the system for an appropriate period per your site guidelines before declaring this maintenance release rollback complete. If all software tests are successful, continue with the next step. Otherwise, if you continue to experience problems with call processing, contact your next level of support or Nortel GNPS.
79	You have completed this emergency rollback procedure.

Troubleshooting maintenance upgrades

If the system becomes unstable after an upgrade or after aborting an upgrade, contact GNPS for assistance.

Patching the NCGL platform

In SN08, only the NCGL platform is patchable.

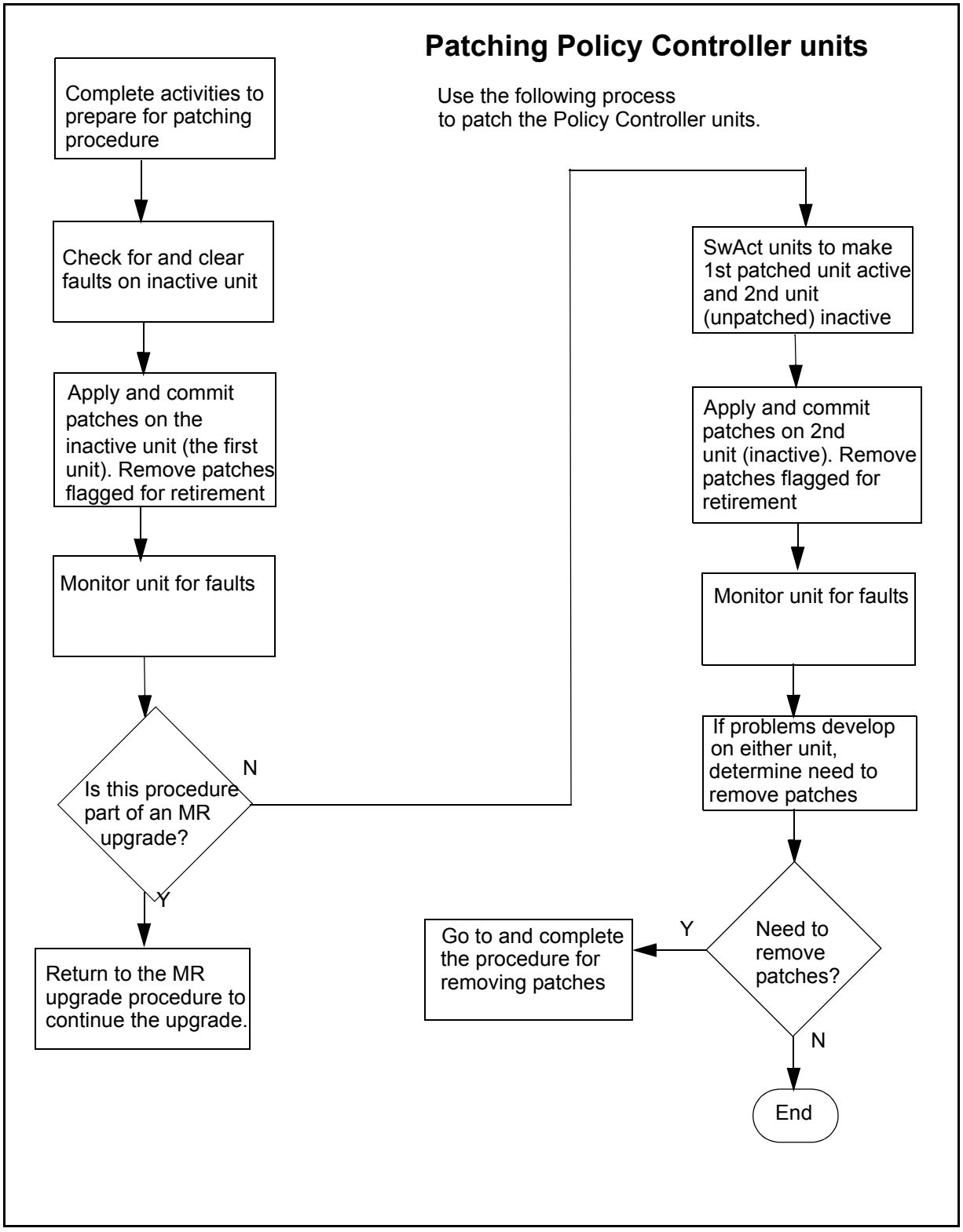
Platform patching activities occur when new patches become available that must be installed. They also occur when an older patch becomes obsolete and must be removed. Installing some patches may be optional.

Patching strategy

Although most patch files apply to any Nortel customer site, some patch files are created for a particular customer's site-specific installation. Not all patches made available apply to all customer sites. Contact Nortel GNPS customer support if you are concerned about which patches are applicable to your site.

Both units in the Policy Controller node must be patched. Each unit is patched separately while it is operating in standby mode. When patching the units, apply and commit the patch to the inactive unit first, then check logs and system status before SwActing the units. Check the logs and status for some period of time to ensure there are no patch-related events. After a time designated by your site guidelines, apply and commit the patch the newly inactive (unpatched) unit and check for logs and system status again.

Refer to the following diagram for a high-level view of the patching process for the Policy Controller units.


Patching Policy Controller units
Use the following process to patch the Policy Controller units.
Complete activities to prepare for patching procedure
Check for and clear faults on inactive unit
Apply and commit patches on the inactive unit (the first unit). Remove patches flagged for retirement
Monitor unit for faults
Is this procedure part of an MR upgrade?
N
Y
Return to the MR upgrade procedure to continue the upgrade.
SwAct units to make 1st patched unit active and 2nd unit (unpatched) inactive
Apply and commit patches on 2nd unit (inactive). Remove patches flagged for retirement
Monitor unit for faults
If problems develop on either unit, determine need to remove patches
Need to remove patches?
Y
Go to and complete the procedure for removing patches
N
End

Patching limitations

Only NCGL Platform patching is supported in SN08. Policy Controller application patches are not supported in SN08.

Patches can only be applied using the CLI (command line interface).

Delivery methods for patch files

Nortel can release NCGL HA patch files at any time. The patch files can also be made available with a major upgrade or during a maintenance release.

You can locate NCGL HA patch files using the following methods:

- From the http://www.nortel.com Web site. Access the Technical Support portal and select Software Downloads. Search under the Carrier VoIP product family for Next Generation Policy Controller.
- From the DVD-ROM software disk, sent to the customer site, that contains the installation software or maintenance release software.
- From a patching CD-ROM sent to the customer site.
- From a customer dropbox service where Nortel delivers patches to a customer-based interface server that is accessible from the internet. The patch files are transferred from the customer-based interface server to the Policy Controller units by the customer network administrator or other trained personnel.

Locating existing patch files on the Policy Controller units

Patch files are stored in the /patching/patchholding directory on each unit that is to be patched.

Prepare for patching activities

Ensure that any critical data such as security certificates and the Policy Controller application database has been backed up to a safe location.

Complete the following steps, in the order indicated, to prepare for patching activities:

Patching preparation

Step	Procedure
80	If you are applying patches while performing a maintenance release upgrade, go to step 83. • If you have purchased security certificates from a Certificate Authority then ensure that you have made a backup copy of the following security certificate files: server.crt, server.crt and certificate.key. These are located in directory /opt/base/share/ssl. • Otherwise, transfer a copy of the default security certificate files (same names and location as above) to a secure location on a remove server. For more information on security certificates for Session Sever refer to the Policy Controller and Administration NTP, NN10434-611.
81	Backup the Policy Controller application database on active unit using procedure *Performing a backup of the Policy Controller database*, found in the Policy Controller Security and Administration NTP, NN10434-611.
82	Acquire patch files from Nortel either using ESD delivery or from a patch or maintenance release DVD-ROM disk.
83	Use procedure View release notes for a maintenance release on page 35 to check release notes to identify the required NCGL patches for your load. Also note any patches that are retired and must be removed.
84	Use procedure Acquire patch files on page 79 to copy the patch files from a DVD to the /patching/patchholding directory. or Use procedure Acquire patch files on page 79 to install patches from a downloaded ISO image, and copy all required patches files from directory /opt/swd/<ESD_ISO_directory>/ to the /patching/patchholding directory.
85	Complete procedure Query status of NCGL patches on page 83

Patching preparation

Step	Procedure
86	Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
87	You have completed this high-level procedure.

Apply and commit patches

Complete the following steps, in the order indicated, to patch both of the Policy Controller units:

Note: This high-level procedure can be part of a high-level maintenance release upgrade procedure.

Patch application

Step	Procedure
88	Complete section Prepare for patching activities on page 26
89	Use procedure Prevent a system SwAct (Jam) on page 39 to jam the units.
90	Complete procedure Apply and commit an NCGL patch on page 87 on the inactive unit.
91	Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
92	If you were directed to this patching from procedure Perform a maintenance release upgrade on page 8, return to that procedure now. Otherwise continue with the next step.
93	Release the JAM on the units using procedure Enable a system SwAct (Unjam) on page 107.

Patch application

Step	Procedure
94	Complete procedure Invoke a maintenance SwAct of the Policy Controller platform on page 103.
95	Use procedure Prevent a system SwAct (Jam) on page 39 to jam the units.
96	Repeat procedure Apply and commit an NCGL patch on page 87 for the second (mate) Policy Controller unit, now the new standby unit.
97	Release the JAM on the units using procedure Enable a system SwAct (Unjam) on page 107.
98	Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
99	You have completed this high-level procedure.

Remove patches

ATTENTION
Under normal operating conditions patches must be removed from both units. Exceptions to this case may be when a patch is being tested on a single unit before being committed and installed on the second unit.

Complete the following steps, in the order indicated, to remove patches from one or both Policy Controller units:

Patch removal

Step	Procedure
100	Use procedure Prevent a system SwAct (Jam) on page 39 to jam the units.
101	Complete procedure Remove an NCGL patch on page 91 on the inactive unit.

Patch removal

Step	Procedure
102	Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
103	Use procedure Enable a system SwAct (Unjam) on page 107 to unjam the units.
104	Complete procedure Invoke a maintenance SwAct of the Policy Controller platform on page 103.
105	Repeat procedure Remove an NCGL patch on page 91 for the second (mate) Policy Controller unit, now the new standby unit.
106	Refer to the Policy Controller Fault Management NTP, NN10438-911, and use procedures *View Policy Controller alarms* and *View Policy Controller logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of the both units before continuing.
107	You have completed this high-level procedure.

Extract an ISO image from an Electronic Software Delivery (ESD)

Purpose of this procedure

Use this procedure to extract an ISO image, patch files and release notes for a maintenance release archive file retrieved from an electronic software delivery dropbox. This procedure may be used as a standalone task or as part of higher level procedure Applying a maintenance release upgrade on page 2.

Prerequisites

Ensure that the ESD software archive file has been transferred from the dropbox on the repository server. The repository server is the machine owned by the operating company that was selected to be the destination for the ESD software files

Your existing Regional Customer Service Team has knowledge of your ESD implementation methodology. You can also contact the technical assistance support (TAS) hotline after hours for any urgent issues related to ESD.

For more information about how your site's ESD is implemented, contact your site network administrator. Also, refer to your solution level Upgrade NTP and the document Electronic Software Delivery Customer Implementation Guide, found on your solution CD.

Restrictions and Limitations

This procedure must be completed on both the active and inactive units.

Action

At a client workstation on the CS-LAN or IEMS client

1 Log onto a Session Server Policy Controller unit using a secure shell by typing

```
> ssh -l <userid> <SS_IP_address>
```

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

SS_IP_address
is the IP address of the Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Change directory to the location of the ESD software archive file by typing

```
$ cd /opt/swd
```

and pressing the Enter key.

6 Ensure that enough disk space is available for the extracted ISO image by typing

```
$ df -k /opt/swd
```

and pressing the Enter key.

The free space on the device is printed. The value for “avail” is the number of free kilobytes. Divide that number by 1000 to determine the number of free megabytes.

7 Uncompress the ESD software load from the ESD archive file by typing

```
$ gunzip <ESD_ISOfilename>.tar.gz
```

and pressing the Enter key.

where

<ESD_ISOfilename>
is a the file name of the ESD delivered MR file

Example
$ gunzip NGSS0070.70.P.NCL.NAP.VAULT.6.D.tar.gz

The ESD software load is uncompressed.

8 Extract the ESD software load from the ESD archive file by typing

`$ gtar -xvf <ESD_ISOfilename>.tar`

and pressing the Enter key.

where

`<ESD_ISOfilename>`
is a the file name of the ESD delivered MR file

Example
$ tar -xvf NGSS0070.70.P.NCL.NAP.VAULT.6.D.tar

The ESD software load is unarchived, and a new directory named after the ESD software filename is created. The directory name is the name of the ESD filename without the .tar.gz suffix. The contents of the ESD software load are placed in this new directory.

9 Change directory to the newly created directory by typing

`$ cd <ESD_ISO_directory>`

and pressing the Enter key.

where

`<ESD_ISO_directory>`
is a the file name of the ESD delivered MR file

Example
$ cd NGSS0070.70.P.NCL.NAP.VAULT.6.D

10 Verify that the image file exists in the directory by typing

`$ ls -l`

and pressing the Enter key.

The system responds with a long listing of files in the directory including the ISO image file, any applicable patch files and the release notes file.

11 This procedure is complete.

View release notes for a maintenance release

Purpose of this procedure

Use this procedure to view the release notes for a maintenance release or patching release. This procedure may be used as a standalone task or as part of a higher level activity.

Limitations and Restrictions

There are no restrictions for performing this procedure.

Prerequisites

If reading release notes from a DVD disk, ensure that the maintenance release DVD-ROM disk is inserted into the inactive unit DVD-ROM drive.

If reading release notes from an ESD delivered ISO archive file, ensure that the software archive file has been extracted and put into the /opt/swd directory on both units using procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 31.

Action

If reading release notes from a DVD disk, proceed with procedure View release notes from a DVD-ROM disk on page 35.

If reading release notes from an ESD delivered ISO archive file, then go to View release notes from an ESD delivered ISO image on page 37.

View release notes from a DVD-ROM disk

At a client workstation on the CS-LAN or IEMS client

1 Log onto the Policy Controller unit using a secure shell by typing

```
> ssh -l <userid> <SS_IP_address>
```

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

SS_IP_address
is the IP address of the Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Verify that the CD/DVD-ROM disk has been inserted into the DVD-ROM disk drive.

6 Mount the DVD-ROM drive by typing

```
$ mount /cdrom
```

and pressing the Enter key.

7 Change directories to the mounted DVD-ROM file system by typing

```
$ cd /cdrom
```

and pressing the Enter key.

8 Locate the release notes file by typing

```
$ ls
```

and pressing the Enter key.

9 Read the contents of the release notes file by typing

```
$ cat <release_notes_filename> | more
```

and pressing the Enter key.

where

<release_notes_filename>
is a file name for the release notes file

10 If necessary use the space bar to page through the contents of the release notes file. If necessary, repeat the previous step to view the contents of the file again.

11 When you are done reviewing the release notes file, change directories out of the mounted DVD-ROM file system by typing

```
$ cd /
```

and pressing the Enter key.

12 Unmount the DVD-ROM drive by typing

```
$ umount /cdrom
```

and pressing the Enter key.

13 You have completed this procedure. Return to step 6 in procedure Upgrade preparation on page 7.

View release notes from an ESD delivered ISO image

At a client workstation on the CS-LAN or IEMS client

1 Log onto the Policy Controller unit using a secure shell by typing

> **ssh -l <userid> <SS_IP_address>**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

SS_IP_address
is the IP address of the Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

$ **su - root**

and pressing the Enter key.

4 When prompted, enter the root password.

5 Change directories to the software directory where the ESD archive file is stored by typing

$ **cd /opt/swd/<ESD_ISO_directory>**

and pressing the Enter key.

where

<ESD_ISO_directory>
is the directory containing the version of the ISO image and release notes that you want to view.

Note: There may be multiple directories containing different versions of ISO images.

6 Locate the release notes file by typing

$ **ls**

and pressing the Enter key.

7 Read the contents of the release notes file by typing

```
$ cat <release_notes_filename> | more
```

and pressing the Enter key.

where

<release_notes_filename>
is a file name for the release notes file

8 If necessary, use the space bar to page through the contents of the release notes file. If necessary, repeat the previous step to view the contents of the file again.

9 You have completed this procedure.

Prevent a system SwAct (Jam)

Purpose of this procedure

The jam command is used to manually prevent a SwAct (switch of activity) of the active and stand-by units by inhibiting the toggling of operational states of both units, thereby preventing the stand-by unit from going active.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as in cases of a replacing a faulty standby unit or upgrading the software for a standby unit.

ATTENTION

You cannot Jam a Policy Controller unit if the inactive unit is out of service.

CAUTION

This procedure prevents the Policy Controller node from operating in a duplex, fault-tolerant mode and prevents the Policy Controller application from being able to SwAct between Policy Controller units as needed. Keep a jam in effect only as long as is necessary.

Prerequisites

There are no prerequisites for performing this procedure.

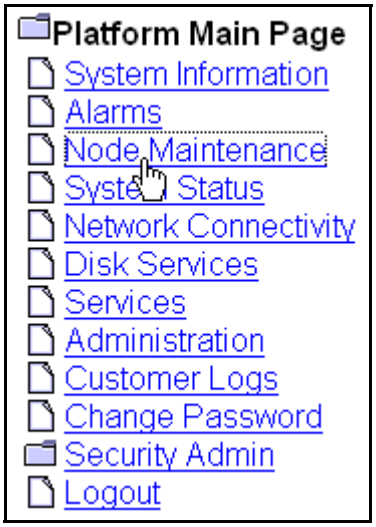
Action

Prevent a system SwAct (Unjam)

At the CS 2000 Session Server Launch Point

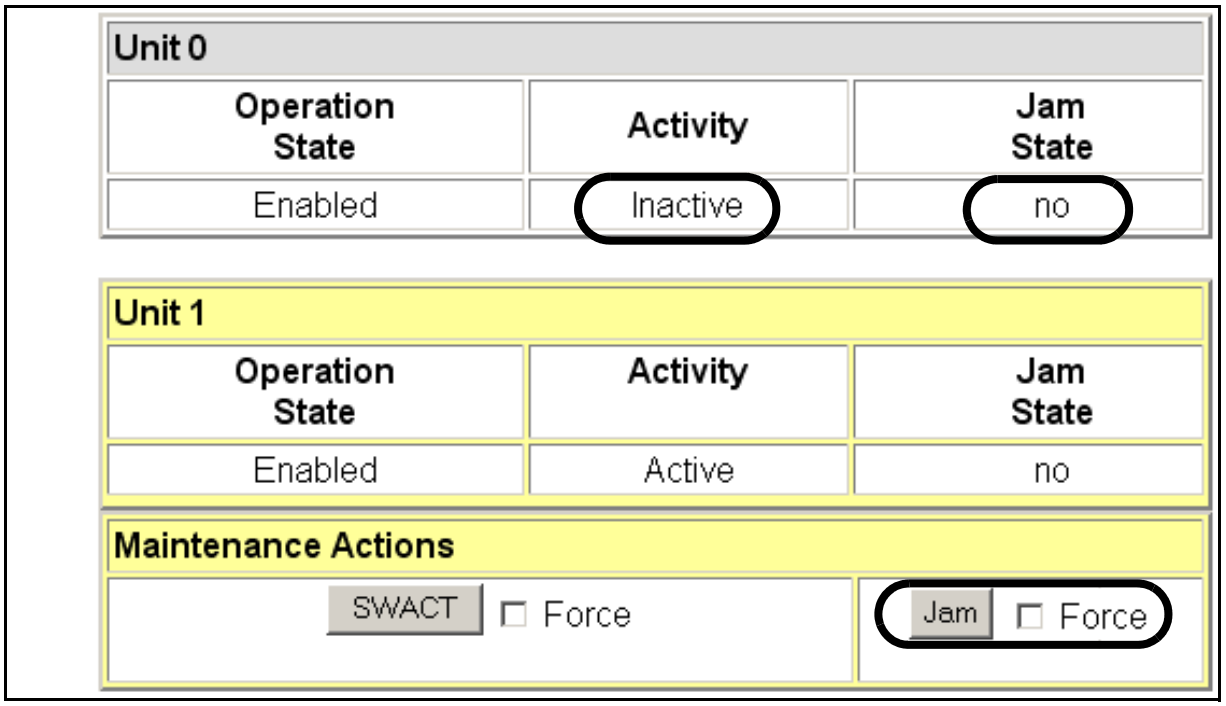
1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

2 Click the **Node Maintenance** link.



The **Node Maintenance** panel displays.

3 Determine if the Jam State of the standby unit is **Yes** or **No**. If it is **Yes**, then the unit is already jammed and you have completed this procedure. If it is **No**, then continue with step 4.



4 Click the **Jam** button.

or

If you want to override any pre-Jam queries, first click the **Force** check box, then click the **Jam** button.

Note: To Jam or Force Jam? The Jam action does not work if critical faults exist on the active unit. Using the Jam command with the Force option overrides any pre-checks. A Forced Jam forces a Jam of the inactive Policy Controller unit even if critical faults exist on the active unit, in which case, a full service outage could occur on the Policy Controller node if the active unit fails.

The system responds

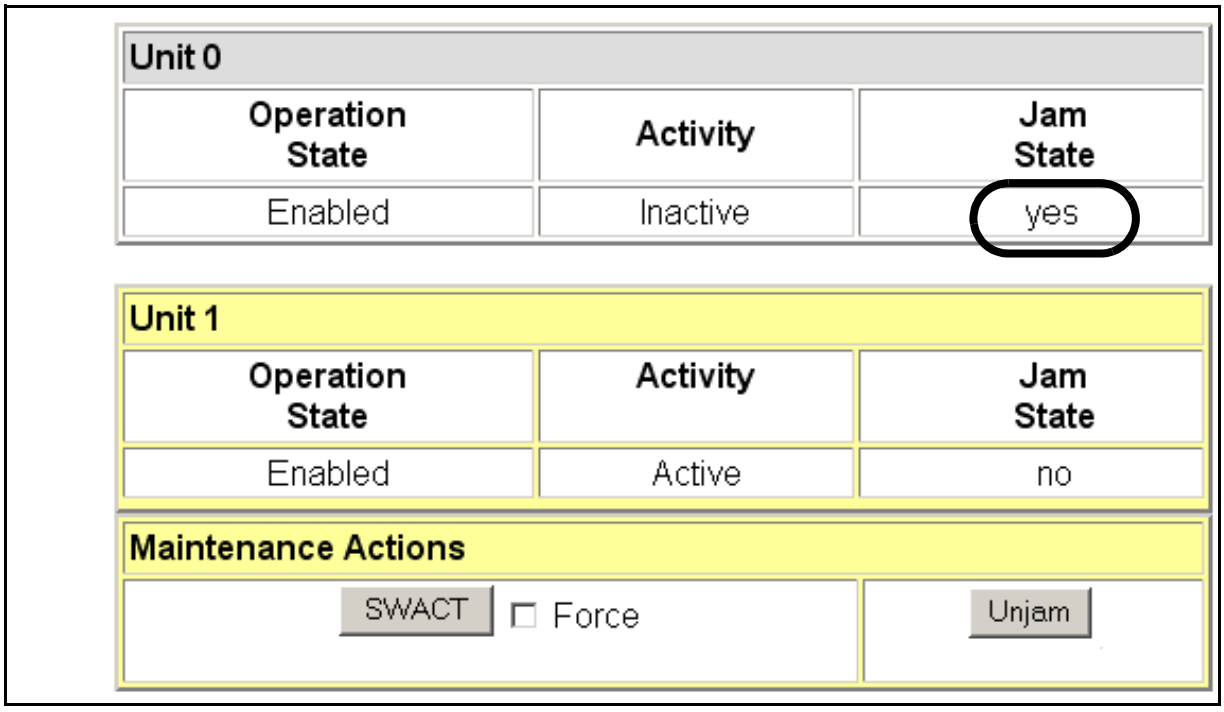
```
Are you sure you wish to perform jam action?

This will prevent the switch of activity to the
inactive node.
Click OK to confirm node jam or cancel to abort.
```

5 Click **OK** to proceed with the jam activity.

The system responds:

```
Info: Jam - Command passed.
```

6 Observe the Jam state for the standby Policy Controller unit transitions from **No** to **Yes**.



7 You have completed this procedure. If applicable, return to Perform a maintenance release upgrade on page 8.

Note: To unjam a standby Policy Controller unit, refer to procedure Enable a system SwAct (Unjam) on page 107.

View the operational status of a Policy Controller NCGL platform

Purpose of this procedure

Use the following procedure to view the service status of the Policy Controller platform hardware and NCGL operating system using the CS 2000 NCGL Platform Manager. Use this procedure as a standalone task or as part of a high-level procedure.

Limitations and restrictions

This procedure provides instructions for determining the service status of the Policy Controller platform only. For instructions on determining the status of the Policy Controller application, refer to procedure View the operational status of the Policy Controller application on page 129.

Although some activities described in this procedure can be accomplished using the CS 2000 Policy Controller Manager, they are described instead using the more complete CS 2000 NGCL Platform Manager.

This procedure does not describe how to change platform or NCGL settings such as changing BIOS settings or platform provisioning.

This procedure does not describe how to view customer logs, alarms or how to change the root password. For detailed instructions on viewing customer logs or alarms, refer to procedures in the Policy Controller Fault Management NTP, NN10438-911. For instructions on how to change the platform root password, refer to the Policy Controller Security and Administration NTP, NN10434-611.

Prerequisites

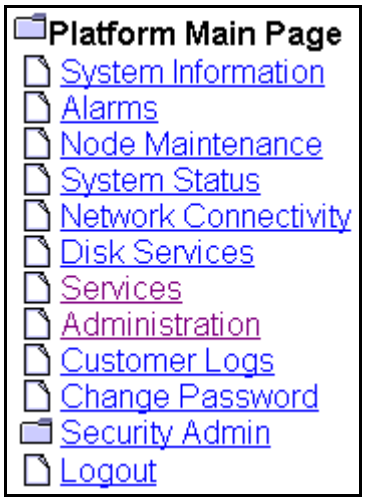
There are no prerequisites for using this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server 2000 NCGL Platform Manager** from the launch point menu.

The **Platform Main Page** menu displays.



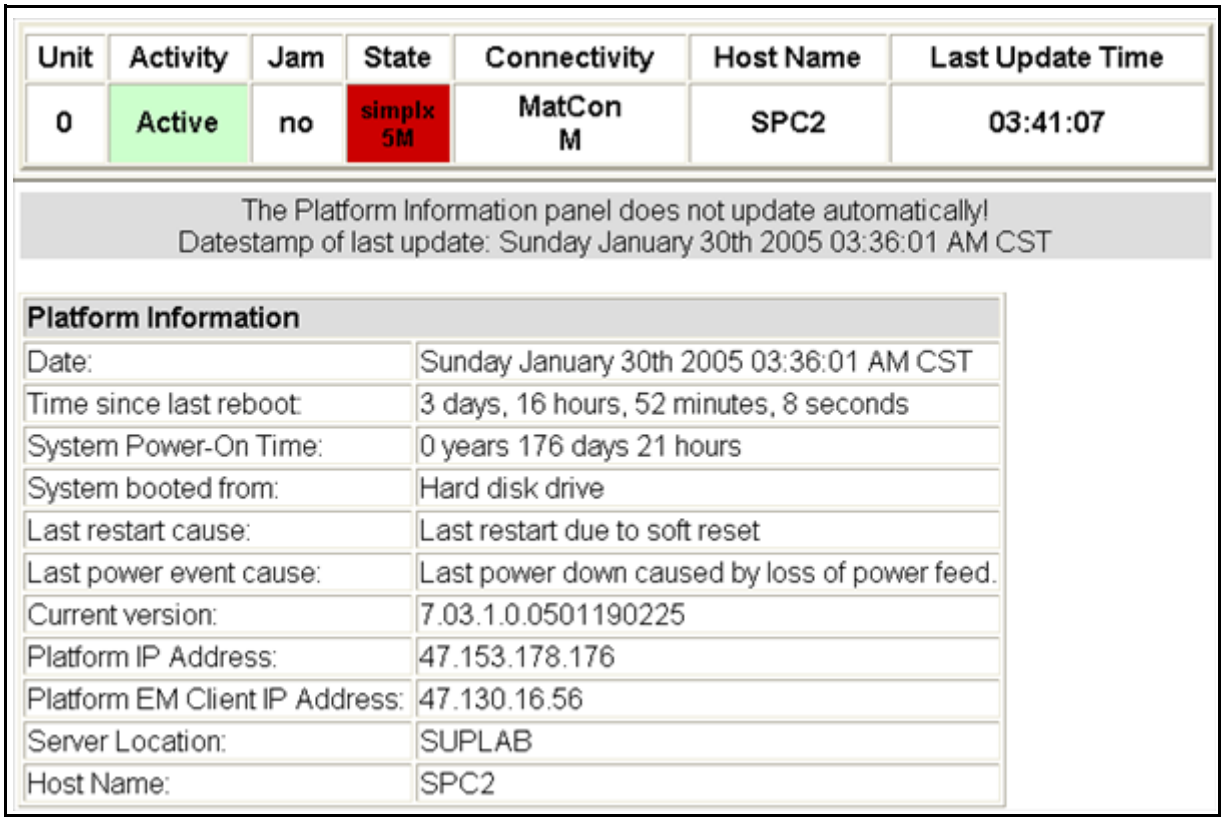
2 From the **Platform Main Page** menu, use the following table to determine your next step.

If	Do
you want to review the version of the platform software load, boot statistics and platform IP address	Click the **System Information** link and go to step 3.
you want to review existing platform alarms	Go to procedure *View Policy Controller alarms* in the Policy Controller Fault Management NTP, NN10438-911.
you want to review node maintenance status	Click the **Node Maintenance** link and go to step 5.
you want to review the status of system processes, CPU load and memory or related alarm thresholds	Click the **System Status** link and go to step 7.
you want to review the connectivity status of the network links. To perform link management activities, refer to the Policy Controller Security and Administration NTP, NN10434-611	Click the **Network Connectivity** link and go to step 9.
you want to review storage related information including array status, disk capacity and disk alarm thresholds	Click the **Disk Services** link and go to step 11.
you want to review details about platform services including the network time protocol servers	Click the **Services** link and go to step 13.
you want to review platform version information only	Click the **Administration** link and go to step 15.
you want to review customer logs	Go to procedure *View Policy Controller logs* in the Policy Controller Fault Management NTP, NN10438-911.
you want to change root passwords	Go to procedure *Manage user passwords with the Policy Controller GUI* in the Policy Controller Security and Administration NTP, NN10434-611.

If	Do
You want to view the security certificate	Go to procedure *View Security Administration information* in the Policy Controller Security and Administration NTP, NN10434-611
you are done reviewing information and want to logout from the GUI	step 17.

3 Review the system information page and use the following table to review the description of the various fields of the Platform (System) Information page.

Note: The Platform (System) Information panel does not update automatically. Click the **System Information** link again to update it.



Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
0	Active	no	simplx 5M	MatCon M	SPC2	03:41:07

The Platform Information panel does not update automatically!
Datestamp of last update: Sunday January 30th 2005 03:36:01 AM CST

Platform Information	
Date:	Sunday January 30th 2005 03:36:01 AM CST
Time since last reboot:	3 days, 16 hours, 52 minutes, 8 seconds
System Power-On Time:	0 years 176 days 21 hours
System booted from:	Hard disk drive
Last restart cause:	Last restart due to soft reset
Last power event cause:	Last power down caused by loss of power feed.
Current version:	7.03.1.0.0501190225
Platform IP Address:	47.153.178.176
Platform EM Client IP Address:	47.130.16.56
Server Location:	SUPLAB
Host Name:	SPC2

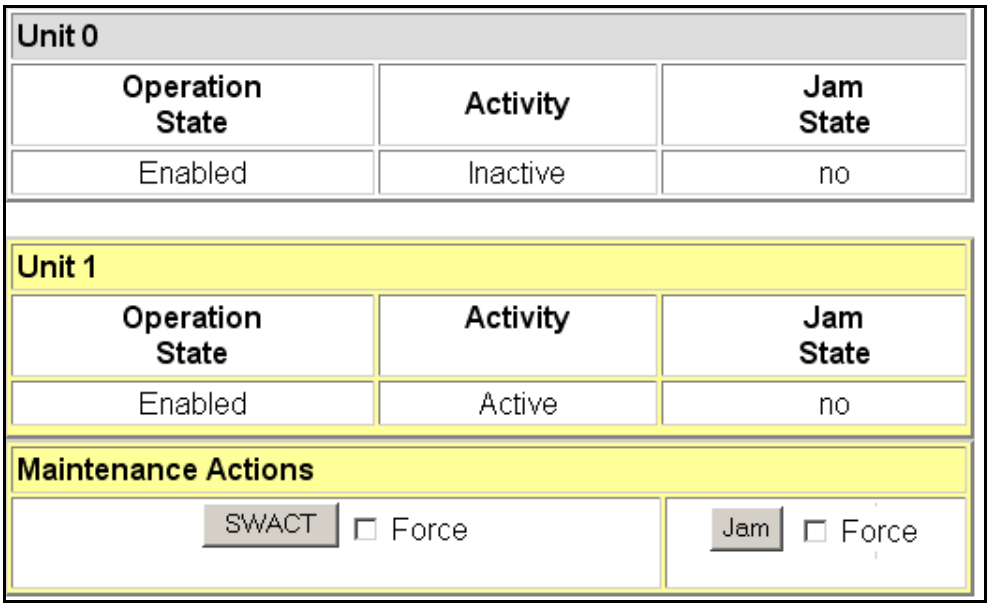
Field	Description
Unit	The Unit number of the Policy Controller in the node that is active. This is the unit you are logged into using your GUI.
Activity	Indicates the activity of the unit (either active or standby).
Jam	Indicates if an activity Jam has occurred on the active Policy Controller unit. This prevents the standby unit from becoming active, regardless of any failures on the active unit.
State	Indicates if the Policy Controller node is operating in a duplex (fault-tolerant) mode or a simplex mode (the standby unit is off-line).
Connectivity	Indicates the state of the network links on the node.
Host Name	Indicates the name of the Policy Controller unit (not node).
Last Update Time	Indicates the last time in hours, minutes and seconds that the Policy Controller unit was updated.
Date	Indicates the system date as maintained by the network time protocol (NTP) server.
Time since last reboot:	Indicates the amount of time that has elapsed since the Policy Controller was last rebooted for any reason.
System Power-On Time:	Indicates the recorded system time that the Policy Controller was powered up.
System booted from:	Indicates whether the Policy Controller is currently booted from the hard drive, or DVD-ROM drive.
Last restart cause:	Indicates any event that forced a platform reboot (manual or system generated).
Last power event cause:	Indicates any event that affected the power supply subsystem of the unit chassis.
Current version:	Indicates the installed version of the Policy Controller platform software. (Does not include the Policy Controller application or other co-resident applications.) Refer to the Upgrading the Policy Controller NTP, NN10431-461, for more procedures on acquiring version information.
Platform IP Address:	Indicates the IP address of the Policy Controller platform.

Field	Description
Platform EM Client IP Address:	Indicates the IP address of the Policy Controller client web interface. This is the IP address of the PC or Unix client from which the GUI was launched. When a web proxy is used, IP address is prefixed with the SSPFS proxy IP address.
Server Location:	Indicates the physical location of the Policy Controller.
Host Name:	Indicates the hostname of the Policy Controller node.

4 When you have completed reviewing **System Information** window, return to step 2.

5 Review the **Node Maintenance** window and use the following table to review the description of the various fields of the Node Maintenance window:

Note: The Node Maintenance panel is refreshed every 45 seconds.



Field	Description
Operation State (unit 0 or 1)	Indicates the operational state of the platform software.
Activity (unit 0 or 1)	Indicates the activity state of the platform software.

Field	Description
Jam State (active unit only)	Indicates whether or not an activity jam has been requested.
Maintenance Actions (active unit only)	Maintenance panel for performing node SwAct activity and to unjam node activity. Refer to the Policy Controller Security and Administration NTP, NN10434-611, for procedures on performing a SwAct or Jam/unJam of the active unit.

6 When you have completed reviewing the **Node Maintenance** window, return to step 2.

7 Review the **System Status** window and use the following table to review the descriptions of the various fields of the System Status page:

Note: The Chassis Information panel is not automatically refreshed.

Chassis Information

Self Test	Chassis Subsystems
Self tests passed.	Chassis subsystems OK.

CPU Load

1 min. load average	5 mins. load average	15 mins. load average	Minor alarm threshold 1 min.	Major alarm threshold 1 min.	Critical alarm threshold 1 min.
0.02	0.01	0.00	10.00	20.00	40.00

CPU Utilization

5 mins. Utilization average	20 mins. Utilization average	30 mins. Utilization average	Minor alarm threshold 5 min.	Major alarm threshold 20 min.	Critical alarm threshold 30 min.
0.77	0.62	0.62	95.00%	99.00%	99.00%

Process Information

Number of processes	Number of zombie process(es)	Zombie		
		Minor alarm threshold value	Major alarm threshold value	Critical alarm threshold value
165	0	5	10	15

Memory Information

Total memory (MB)	Free memory (MB)	Available memory (MB)	Minor alarm threshold value (MB)	Major alarm threshold value (MB)	Critical alarm threshold value (MB)
3,787.31	2,951.86	3,539.29	500.00	250.00	100.00

Field	Description
Chassis information: Self Test	Indicates the status of the self test performed on the platform at boot up.
Chassis information: Chassis Subsystems	Indicates the status of the platform hardware subsystems including the memory, CPU, all drives, network connection, power supplies, cooling and other I/O connections.
CPU Information: load average	Indicates the 1, 5 and 15 minute load averages for the CPU utilization.
CPU information: load average threshold values	Indicates the 1 minute CPU load average utilization threshold value. When the set threshold value is exceeded, the appropriate minor, major or critical alarm is raised.
Chassis Utilization: Utilization average	Indicates the 5, 20 and 30 minute CPU utilization average. When the threshold value is exceeded, an alarm is raised.
Chassis Utilization: alarm threshold values	Indicates the 5, 20 and 30 minute CPU utilization average threshold value. When the set threshold value is exceeded, an alarm is raised.
Process Information: Number of Processes	Indicates the total number of processes (non-threaded) that are running on the Policy Controller Platform.
Process Information: Number of zombie processes	Indicates the number of defunct or terminated NCGL zombie processes. ***Note:*** A zombie process is a process that has terminated either because it has been killed by a signal or because it has called an exit() and whose parent process has not yet received notification of its termination. A zombie process exists solely as a process table entry and consumes no other resources.
Process Information-zombie: minor alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a minor alarm is raised indicating that the set threshold has been exceeded.

Field	Description
Process Information-zombie: major alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a major alarm is raised indicating that the set threshold has been exceeded.
Process Information-zombie: critical alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a critical alarm is raised indicating that the set threshold has been exceeded.
Memory Information: Total Memory (MB)	The total amount of RAM installed on the motherboard of each Policy Controller unit. Both units must have the same amount.
Memory Information: Free Memory (MB)	The amount of memory available unallocated for use.
Memory Information: Available memory (MB)	The amount of memory available for programs.
Memory Information: minor alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a minor alarm is raised.
Memory Information: major alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a major alarm is raised.
Memory Information: critical alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a critical alarm is raised.

8 When you have completed reviewing the System Status, return to step 2.

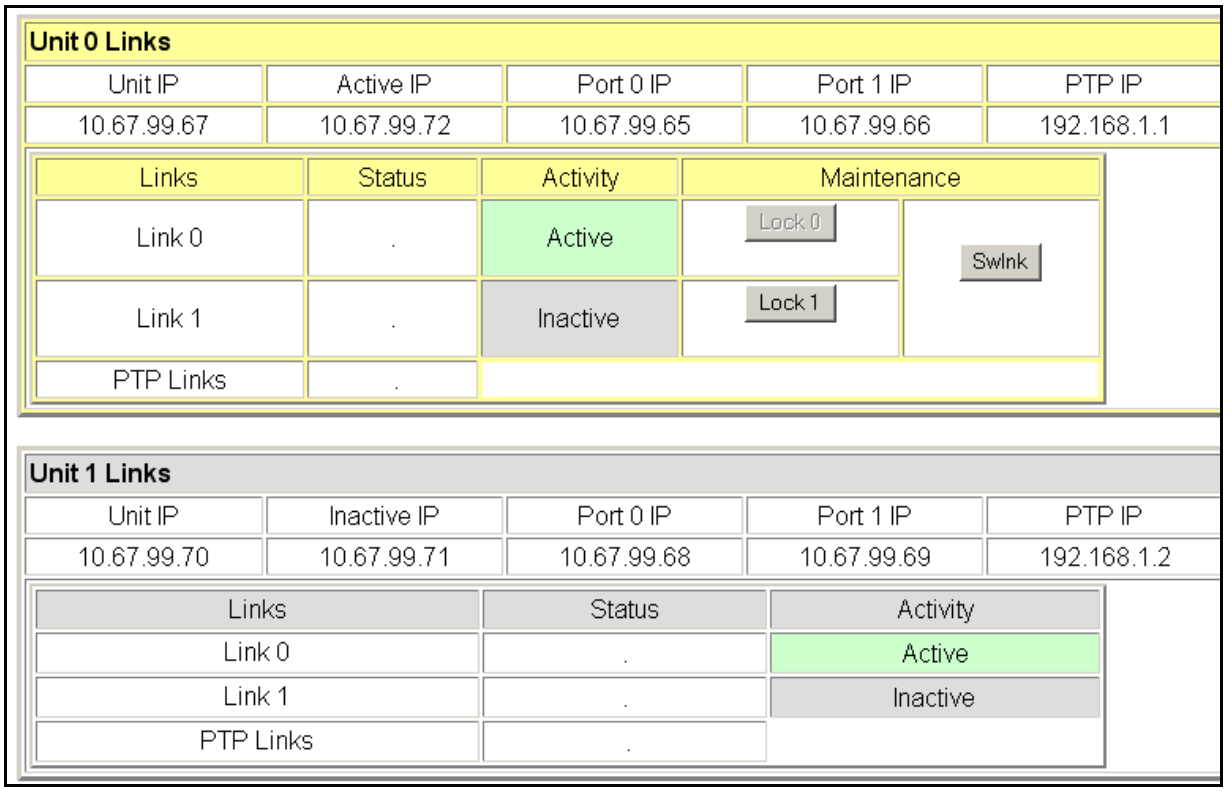
9

ATTENTION

Do not perform link management activities such as Lock, Suspend or Swlink using this procedure. Refer to the Policy Controller Security and Administration NTP, NN10434-611, to perform these activities.

Review the **Network Connectivity** window and use the following table to review the description of the various fields of the Network Connectivity page:

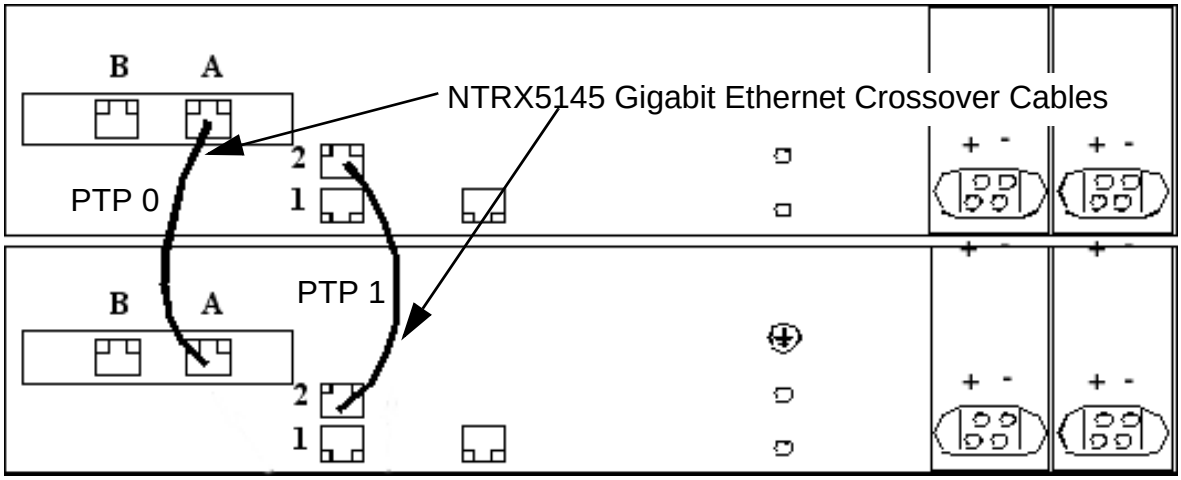
Note: The Network Connectivity panel is refreshed every 45 seconds.



Field	Description
Unit 0,1 Links	Indicates which ethernet IP links are installed on the Policy Controller units (each unit has two links).
Unit 0,1 Status	Indicates the status of the ethernet links.

Field	Description
Unit 0,1 Activity	Indicates the activity status of the ethernet links; either active or inactive.
Unit 0,1 Maintenance	Indicates the maintenance actions that can be performed on the ethernet links; either Lock, Unlock or Swlink. Refer to NTP *Policy Controller Security and Administration*, NN10434-611, to perform link management.
Unit 0,1 PTP Links status	Indicates the status of the PTP links between both units in the node.
Unit IP	The network IP address of the Policy Controller unit.
Active IP	The IP address of the local (active) Policy Controller unit.
Inactive IP	The IP address of the mate (inactive) Policy Controller unit.
Port 0 IP	The IP address of the active or inactive ethernet port 0.
Port 1 IP	The IP address of the active or inactive ethernet port 1.
PTP IP	The IP address of the active or inactive PTP link.

Crossover and LAN ethernet cable connections for Policy Controller units



Ethernet Ports:

Ports 1 and B (both sets) go to CS-LAN Switch

Ports 2 (PTP1) and A (PTP0) are point-to-point connections between Policy Controller units

10 When you have completed reviewing the Network Connectivity files, return to step 2.

11 Review the **Disk Services** window and use the following table to review the description of the various fields of the Disk Storage page:

Note 1: The Disk Services panel does not update automatically. Click the **Disk Services** link again to update it.

Note 2: To create and remove file systems, refer to applicable procedures in the Policy Controller Configuration Management NTP, NN10432-511.

RAID Array Status

Name	Size (GB)	State	Disk 0	Disk 1	Status
/boot	0.10	.	.	.	Array is operating normally
ntvg	68.26	.	.	.	Array is operating normally

Disk Maintenance

Disk Number	Disk Size (GB)	Disk State	Disk Action
0	68.37	.	Remove
1	68.37	.	Remove

Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	Total Space Available (MB)	Total Space Available (%)	Minor Alarm Threshold (%)	Major Alarm Threshold (%)	Critical Alarm Threshold (%)
	/	.	61.47	58.29	100.00	0.00	0.00	85.00	90.00	95.00
No	/boot	.	98.65	19.08	21.00	74.48	79.00	-	-	-
Yes	/opt/base	.	699.31	0.46	1.00	698.85	99.00	85.00	90.00	95.00
No	/opt/apps	.	507.31	314.31	62.00	193.00	38.00	-	-	-
Yes	/tmp	.	123.31	0.31	1.00	123.00	99.00	85.00	90.00	95.00
Yes	/var/log	.	507.31	9.61	2.00	497.71	98.00	85.00	90.00	95.00
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00	-	-	-
No	/opt/apps/webint	.	1,494.00	209.78	15.00	1,284.22	85.00	-	-	-
No	/opt/apps/database	.	10,006.00	48.19	1.00	9,957.81	99.00	-	-	-
No	/opt/apps/logs	.	507.31	206.34	41.00	300.98	59.00	-	-	-
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00	-	-	-

Create/Remove Filesystem

Create New Filesystem | Remove Filesystem

Volume Group Information

Volume Group Name	Volume Group Size (GB)	Total Space Allocated (GB)	Total Space Allocated (%)	Total Space Available (GB)	Total Space Available (%)
ntvg	68.22	23.84	34.95	44.38	65.05

Field	Description
RAID Array Status: Name	Indicates the name of each RAID-1 array in the system.
RAID Array Status: Size (GB)	Indicates the size of the partition in gigabytes.

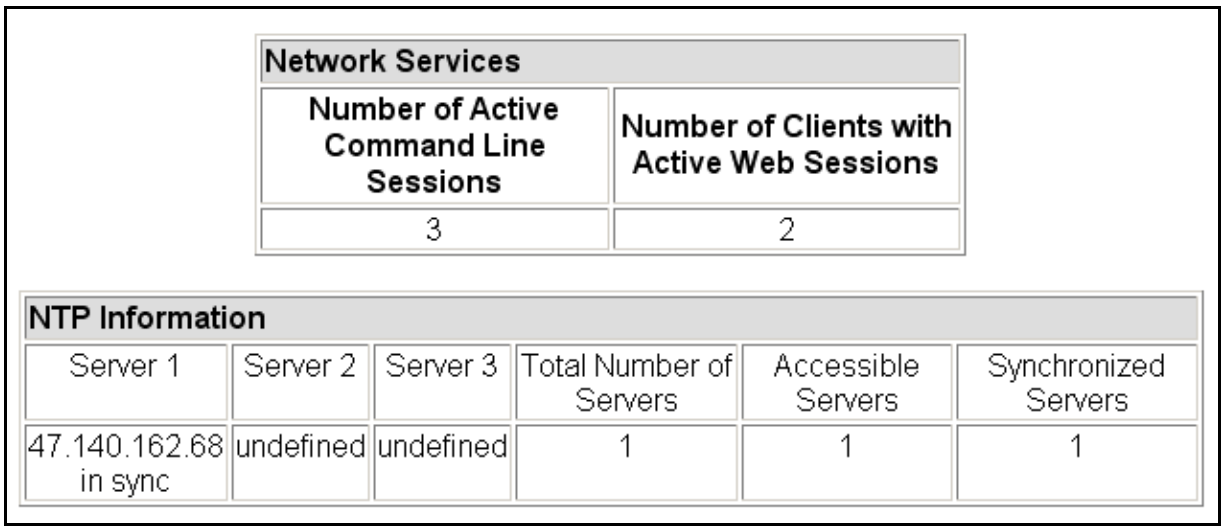
Field	Description
RAID Array Status: State	Indicates a high level state for the array: - ".": indicates the array is functioning normally. - Missing: a disk was removed from the array. - Failed: a disk in the array has failed and needs to be replaced. -Rebuilding: the array is in the process of rebuilding to a fault-tolerant mode.
RAID Array Status: Disk 0	Indicates the service status of disk 0.
RAID Array Status: Disk 1	Indicates the service status of disk 1.
RAID Array Status: Status	Indicates the status of the array. Values are: - The array is operating normally - Missing - Failed - Rebuild.
Disk Maintenance: Disk Number	Indicates the disk number in the array; 0 or 1.
Disk Maintenance: Disk Size (GB)	Indicates the total capacity of the disk drive in gigabytes.
Disk Maintenance: Disk State	Indicates the installation state of the disk.
Disk Maintenance: Disk Action	Indicates whether a hard disk can be inserted into the operating system. For more information about the **Remove** and **Insert** commands, refer to the Upgrading the Policy Controller NTP, NN10431-461.
Filesystem Information: Monitor	Indicates the status of individual file systems on the disk array. For more information about the **Monitor** command, refer to procedures in the Policy Controller Configuration Management NTP, NN10432-511.
Filesystem Information: Filesystem Name	Indicates the name of the filesystem on the disk array. Some filesystem names are reserved.
Filesystem Information: Test Results	Indicates the results of any tests run on the filesystems. Tests are run approximately every 10 minutes to verify that all of the basic filesystem operations are working on each of the filesystems.
Filesystem Information: Total Space (MB)	Indicates the total amount of disk space (in MB) allocated for this filesystem.

Field	Description
Filesystem Information: Total Space Used (MB)	Indicates the total amount of disk space (in MB) in use on this file system.
Filesystem Information: Total Space Used (%)	Indicates the total amount of disk space (in %) in use on this file system.
Filesystem Information: Total Space Available (MB)	Indicates the percent of total disk space (in MB) free for use on this filesystem.
Filesystem Information: Total Space Available (%)	Indicates the amount of disk space (in %) available for use by platform processes and applications.
Filesystem Information: Minor Alarm Threshold (%)	Indicates the maximum amount of disk space (in percent) that can be utilized before a minor alarm is raised indicating that the set threshold has been exceeded.
Filesystem Information: Major Alarm Threshold (%)	Indicates the maximum amount of disk space (in percent) that can be utilized before a major alarm is raised indicating that the set threshold has been exceeded.
Filesystem Information: Critical Alarm Threshold (%)	Indicates the maximum amount of disk space (in percent) that can be utilized before a critical alarm is raised indicating that the set threshold has been exceeded.
Volume Group Information: Volume Group Name	Indicates the name of the volume group in the array.
Volume Group Information: Volume Group Size (GB)	Indicates the total size of the volume group in the array.
Volume Group Information: Total Space Allocated (GB)	Indicates the amount of volume group space, in gigabytes, currently allocated to filesystems.
Volume Group Information: Total Space Allocated (%)	Indicates the amount of volume group space (in %) currently allocated to file systems.
Volume Group Information: Total Space Available (GB)	Indicates the amount of unallocated volume group space, in gigabytes, available for filesystems.
Volume Group Information: Total Space Available (%)	Indicates the amount of unallocated volume group space (in %) available for file systems.

12 When you have completed reviewing the Disk Services page, return to step 2.

13 Review the Services page and use the following table to review the description of the various fields of the Platform Services page:

Note: The Services panel does not update automatically. Click the **Services** link again to update it.



Network Services	
Number of Active Command Line Sessions	Number of Clients with Active Web Sessions
3	2

NTP Information					
Server 1	Server 2	Server 3	Total Number of Servers	Accessible Servers	Synchronized Servers
47.140.162.68 in sync	undefined	undefined	1	1	1

Field	Description
Network Services: Number of Active Command Line Sessions	Indicates the number of command line interface (CLI) sessions (both remote and local) on the Policy Controller.
Network Services: Number of Clients with Active Web Sessions	Indicates the number of clients running one or more web GUI sessions.
NTP Information: Server1 - Server 3	Indicates the IP address of up to 3 Network Time Protocol (NTP) servers in the network, along with the status of the connection.
NTP Information: Total Number of Servers	Indicates the number of NTP servers registered with the CS-LAN network.
NTP Information: Accessible Servers	Indicates the number of NTP servers accessible to the Policy Controller.
NTP Information: Synchronized Servers	Indicates the number of NTP servers to which the Policy Controller is synchronized.

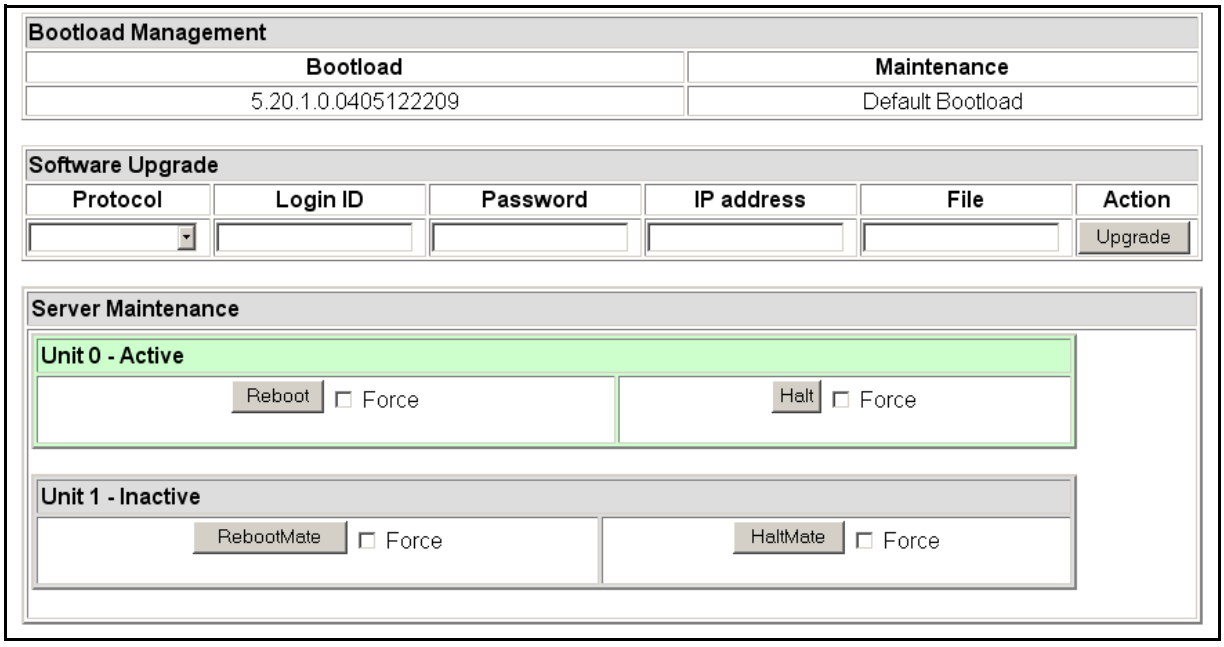
14 When you have completed reviewing Platform Services status, return to step 2.

15 Review the Administration page and use the following table to review the description of the various fields of the Platform Admin page:

Note: The Administration panel does not update automatically. Click the link again to update it.

ATTENTION

To perform software upgrades to the NCGL platform, refer to NTP *Upgrading the Policy Controller*, NN10431-461.



Field	Description
Bootload Setting: Bootload	Indicates the load ID for the NCGL platform software load.
Bootload Setting: Maintenance	Indicates whether the Bootload is the default. May also allow choosing a new default bootload if there is more than one load available. Additional loads can come from maintenance releases.

Field	Description
Software Upgrade: Protocol	Indicates the file transfer protocol or source location for the platform software upgrade: FTP, Anonymous FTP, HTTP, HTTPS, Local File, Local CDROM.
Software Upgrade: Login ID	If a login ID is required to access the upgrade platform load from another server in the network, a login ID can be entered here.
Software Upgrade: Password	If a password is required to access the upgrade platform load from another server in the network, a password can be entered here.
Software Upgrade: IP Address	If it is required to access the upgrade platform load from another server in the network, an IP address can be entered here.
Software Upgrade: File	The target upgrade load path and filename is entered here.
Software Upgrade: Action Upgrade button	The **Upgrade** button initiates a platform NCGL upgrade. Refer to Upgrading the Policy Controller Upgrades, NN10431-461, for instructions on using this function.
Server Maintenance (active and inactive units)	To execute the **Reboot**, **Halt**, **Rebootmate** and **Haltmate** functions, refer to the applicable procedures in the Policy Controller Security and Administration NTP, NN10434-611.

16 When you have completed reviewing Platform Admin page, return to step 2, or continue with step 17.

17 If you want to logout from platform GUI, click the **Logout** link.

You are returned to the login page.

18 You have completed this procedure. If applicable, return to Perform a maintenance release upgrade on page 8.

Determine the current version of software loads

Purpose of this procedure

Use this procedure to do the following tasks:

- Determine the version of the software for the Policy Controller application on the Active unit.
- Determine the version of the software for the NGGL platform on the Active unit only if a maintenance release has not been applied.
- Use it as a standalone task or as part of a higher level activity.

Limitations and Restrictions

Applying a maintenance release to the NGGL platform load causes inaccurate NGGL platform version information to show in the **Version Information** window. Use this procedure to view the NGGL platform version only if a maintenance release has not been applied to the NGGL platform load.

If a maintenance release has been applied to the NCGL platform load, determine the NCGL platform load version by using procedure View the operational status of a Policy Controller NCGL platform on page 43 and go to the ***System Info*** window.

Prerequisites

This procedure has no prerequisites.

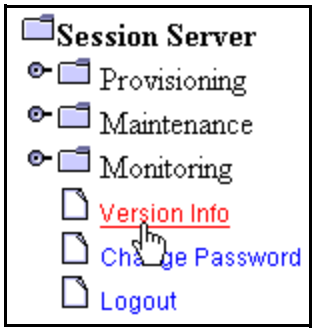
Action

Determine the current version of the software load

At an Integrated EMS or client workstation

1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.

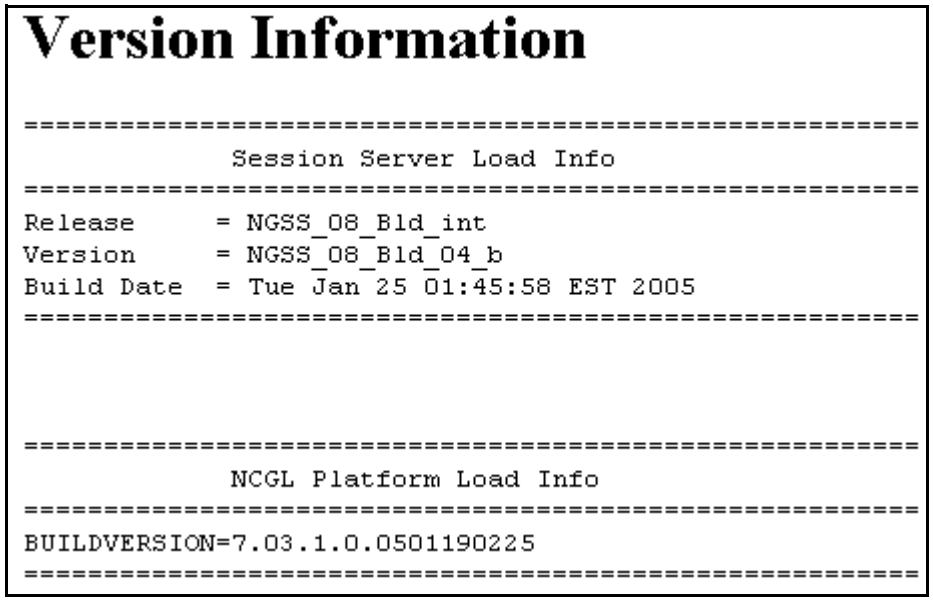
2 At the **Session Server** folder, click the **Version Info** link.



The **Version Information** window displays.

3 Review and record the load version information for the Policy Controller application or the NGGL platform.

Note: The version information for the NCGL platform load is only accurate if a maintenance release has not been applied to the load. If a maintenance release has been applied to the NCGL platform load, the version information is not accurately reflected in this window.



4 You have completed this procedure.

Upgrade Policy Controller NCGL platform software

Purpose of this procedure

This procedure describes how to use the CS 2000 NCGL Platform Manager GUI to apply (upgrade) a maintenance release to an NCGL platform load.

ATTENTION
This procedure should only be used as part of the high level activity Perform a maintenance release upgrade on page 8.

Limitations and Restrictions

You can upgrade the NCGL platform load from the local DVD-ROM drive, from an ISO image located on the system disk drive, or from a Policy Controller DVD data disk mounted elsewhere in the network (via FTP). The following upgrade protocols (methods) are selectable from the CS 2000 NCGL Platform Manager GUI:

- Local CDROM - the local DVD-ROM drive (labelled as the local CD-ROM)
- Local file - an iso image, or load.tgz file copied from the local DVD-ROM drive copied to the hard drive using the secure copy program, **scp**, to transfer the data
- Remote file using FTP or anonymous FTP - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the FTP service. If the workstation or server is configured to allow anonymous FTP, use anonymous FTP to avoid sending username and password information in clear text format across the network.
- Remote file using HTTP or HTTPS - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP or HTTPS service.

Prerequisites

When upgrading, first refer to section Upgrade preparation on page 7 for the prerequisites of performing a maintenance release.

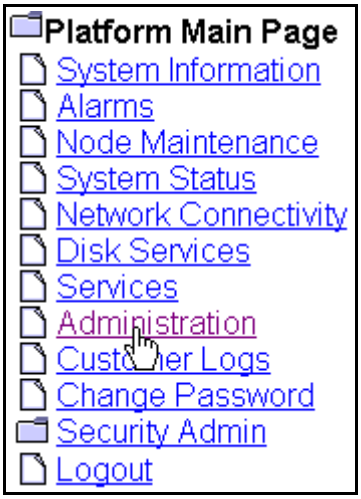
Action

At the CS 2000 Session Server Launch Point

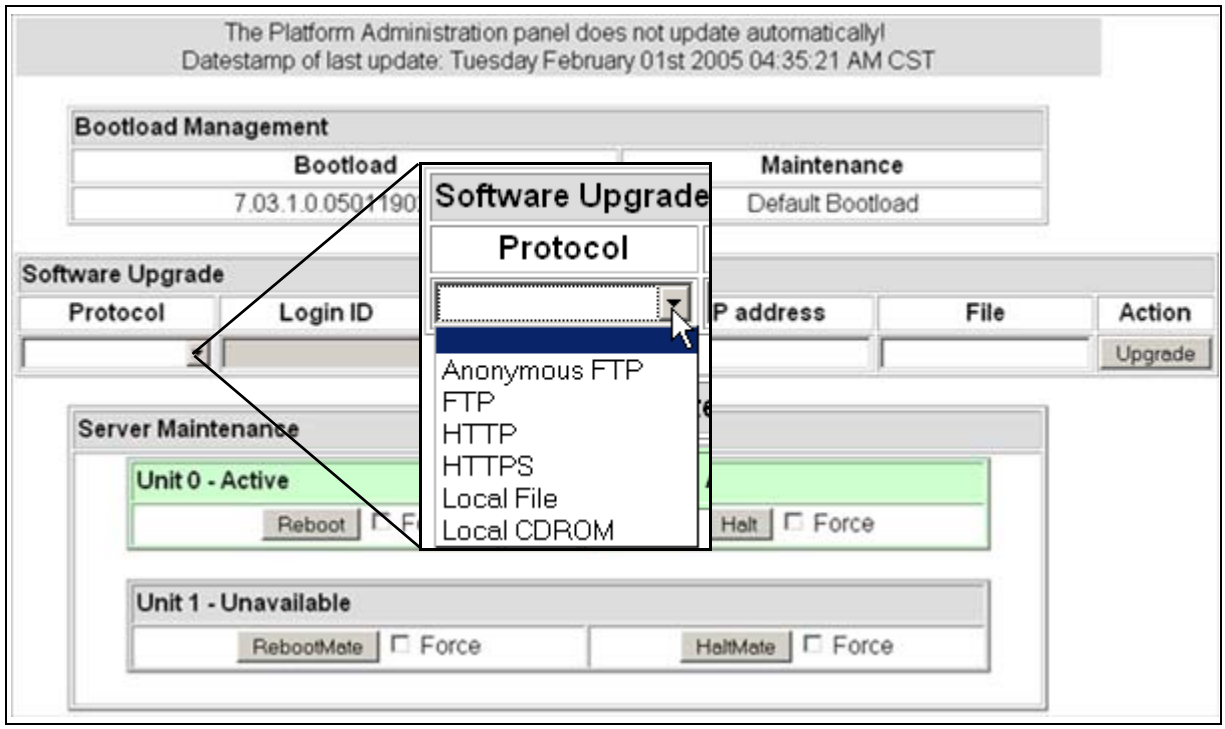
1 Select **Succession Communication Server 2000 NCGL Platform Manager** from the launch point menu.

The **Platform Main Page** menu displays.

2 Click the **Administration** link.



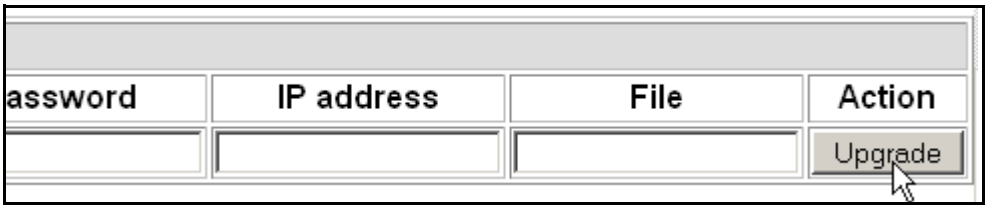
3 Click the **Protocol** drop down menu and select an upgrade protocol. Refer to the following table to help you determine the appropriate protocol:



If the Protocol is	Do
Anonymous FTP	Enter the IP address of the remote server which has the bootload image in the IP address text box. Enter the location (as a relative path on the remote server) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`. then continue with step 4

If the Protocol is	Do
FTP	Enter your username in the Login ID text box. Enter your password in the Password text box. Enter the IP address of the remote server which has the bootload image in the IP address text box. Enter the location (as a relative path) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`. then continue with step 4
HTTP or HTTPS	Enter the IP address of the remote server which has the bootload image in the IP address text box. Enter the location (as a relative path on the remote server) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`. then continue with step 4
Local File	Enter the location (as a relative path of the Policy Controller unit) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`. then continue with step 4
Local CDROM	Ensure that the DVD-ROM disk is inserted into the drive then continue with step 4

4 Click the **Upgrade** button.



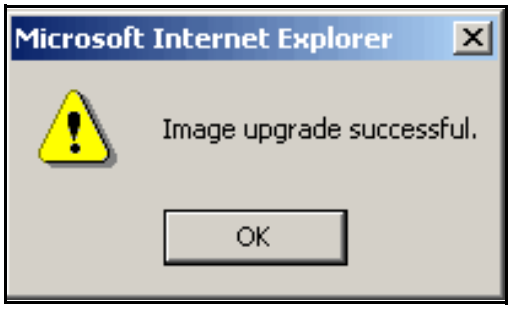
A popup window appears indicating the success of the upgrade.

5

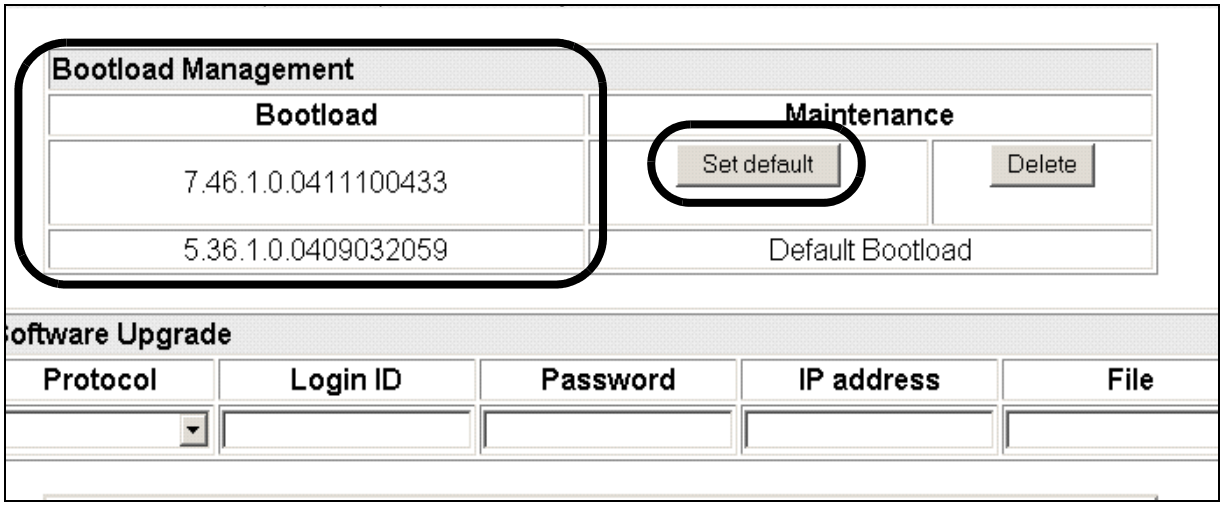
ATTENTION

Click OK on the popup window to continue. Once complete, you will be able to verify the files were successfully copied. Refer to the Troubleshooting on page 71 section if you encounter problems.

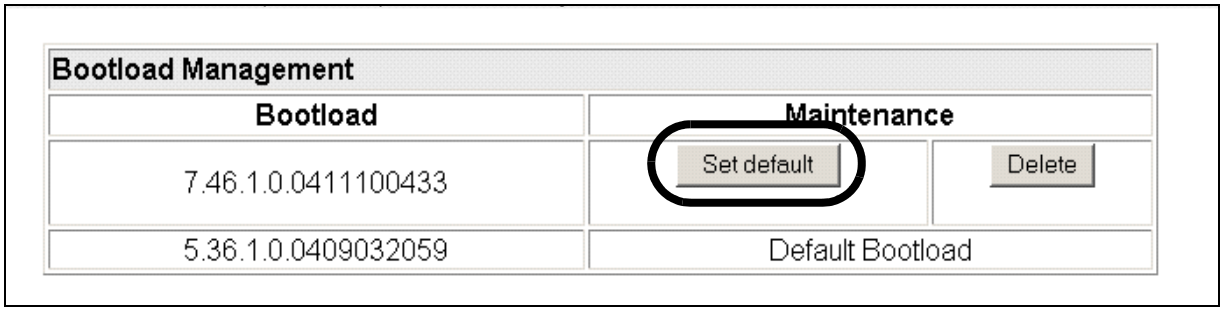
Verify that the load files were successfully copied by clicking **OK** on the popup window.



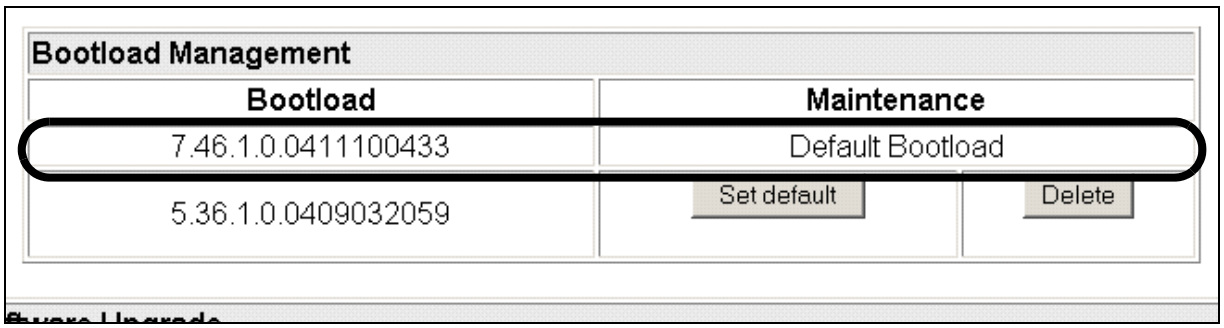
6 When the selected NCGL load has been successfully copied to the unit, look for the load name to appear in the Bootload Management panel.



7 Click the **Set Default** button to the right of the new (upgraded) bootload.



The system responds by setting the newly installed load as the default load, as shown below.



8 Verify that you have set the correct bootload to be the default.

9 If you upgraded using the Local CD-ROM protocol, remove the DVD-ROM disk from the drive.

10 You have completed this procedure. If you were forwarded to this procedure from another procedure, return to that procedure and continue with the steps.

Troubleshooting

For step 5 of this procedure, review the message in the popup window. The following possible error messages and their meaning are described:

- Error: Failed to update image /usr/bin/copy_boot_image -f /opt/swd/load.tgz Invalid load file content. Exiting

  Indication: If the bootload file is corrupt, the system software indicates that the bootload contains invalid content.

- Error: Failed to update image /usr/bin/copy_boot_image -u https://10.40.5.62//tmp/load.tgz: Failed to retrieve file from the network.

  Indication: The user has attempted to perform software upgrade where the file path or the IP address used is not correct. You need

to validated that the IP address is correct, also, make sure the file path is correct.

- Error: Failed to update image /usr/bin/copy_boot_image -u ftp://mtc:mtc@10.40.5.59//usr/load.tgz: Failed to retrieve file from the network.

  Indication: The user has attempted to perform software upgrade where the file path or the user ID or password used is not correct. You need to validated that the file path is correct and make sure to check the user ID and password.

- Error: Failed to update image /usr/bin/copy_boot_image -u ftp://mtc:mtc@10.40.5.59//usr/load.tgz: 10.40.5.59 IP address is not responding.

  Indication: The user has attempted to perform software upgrade from a host that is not responding. You need to check that the host IP address is available and try again.

- Error: Failed to update image /usr/bin/copy_boot_image -f load.tgz: Could not find load.tgz

  Indication: The user has attempted to perform software upgrade where the file path is not correct. Validate that the file path is correct.

- Error: Failed to update image /usr/bin/copy_boot_image -c: Failed to mount the cdrom RC=32

  Indication: If the CDROM is not placed in the CDROM drive and an attempt is made to upgrade software with the “Local CDROM” option, the following message window appears. Verify that the CDROM is in the drive. If the CDROM is inserted, verify that the drive is functioning properly.

  or

  The user has attempted to perform a software upgrade where there is a problem with mounting the CD-ROM drive. Mount or remount the CD-ROM drive before attempting another software upgrade process.

- Error: Failed to update image /usr/bin/copy_boot_image -u https://10.40.5.62/load.tgz: Unable to decompress /opt/base/upgrade/29335/load.tgz Exiting

  Indication: The user has attempted to perform software upgrade, which uses filesystem (/opt/base) that is full. You need to remove unwanted files and make sure there is enough space in the targeted filesystem.

Reboot a Policy Controller unit

Purpose of this procedure

Use this procedure to perform a graceful shut down and reboot of the NCGL operating system running on a Policy Controller unit. Use this procedure only as part of a high-level activity such as part of maintenance or fault clearing activities or part of a software upgrade activity.

ATTENTION

This procedure causes a 3-4 minute service interruption of the affected unit and should only be used when recommended by Nortel support personnel.

Limitations and restrictions

ATTENTION

Nortel Networks recommends performing this procedure only on the standby unit.

CAUTION

If both the active and inactive units are rebooted, the reboot procedure prevents the Policy Controller from performing Virtual Call Admission Control processing. If the inactive unit alone is rebooted, then this prevents the Policy Controller node from operating in a fault-tolerant state.

***Note**:* The CS 2000 will still process calls without VCAC if it determines the Policy Controller is unreachable.

You cannot reboot an active unit in duplex mode. A rebootmate is the only command that will work in duplex mode.

Prerequisites

Use procedure View the operational status of a Policy Controller NCGL platform on page 43 to verify any disk array rebuilds in progress, by checking the Alarms on the Policy Controller. Wait for the rebuild to complete before executing this procedure.

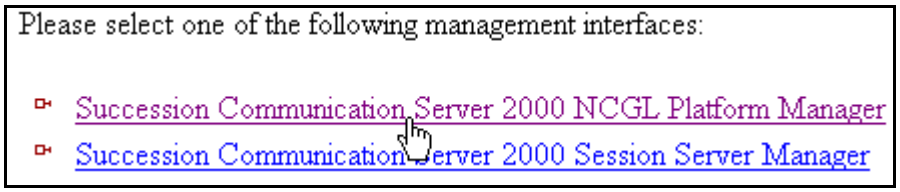
Ensure that you have your bootable software installation DVD disk available, in case you have trouble rebooting the unit.

Action

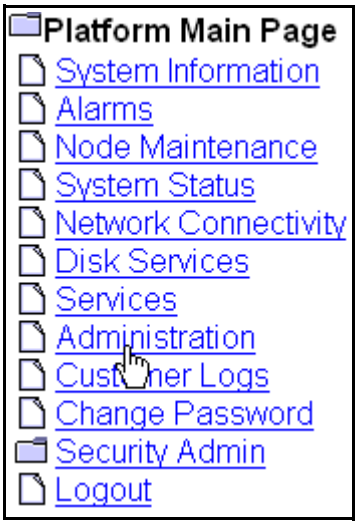
Reboot a Policy Controller Unit

At the CS 2000 Session Server Launch Point

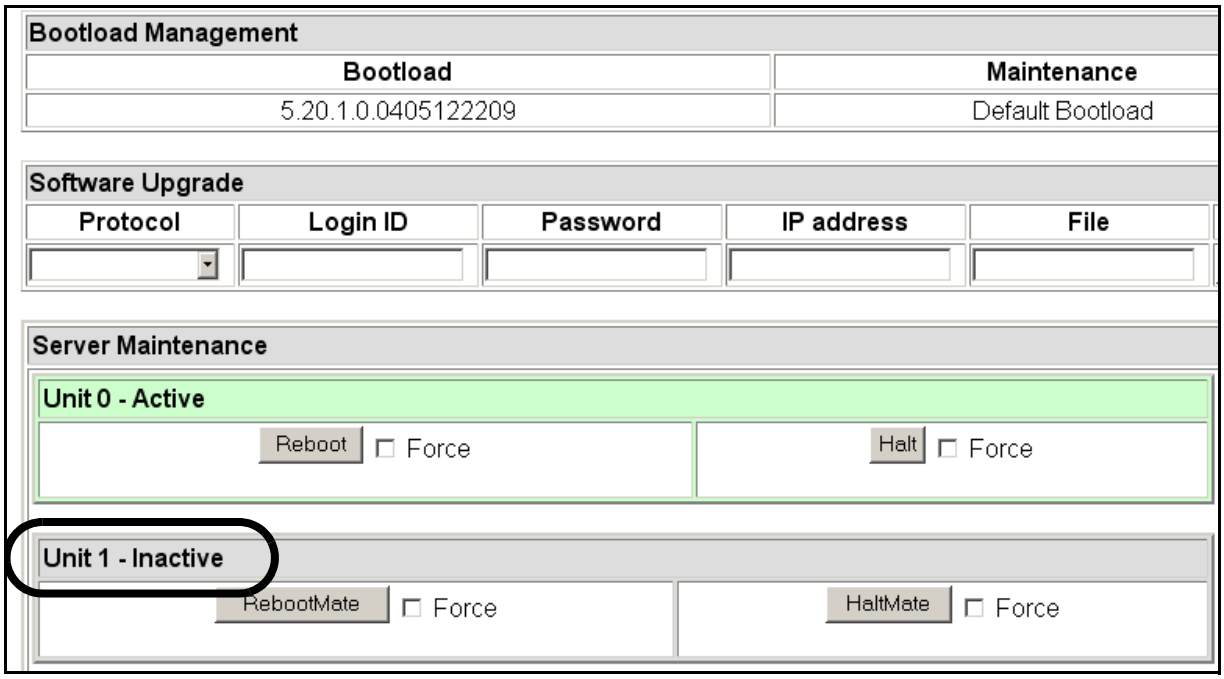
1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



2 Click the **Administration** link.



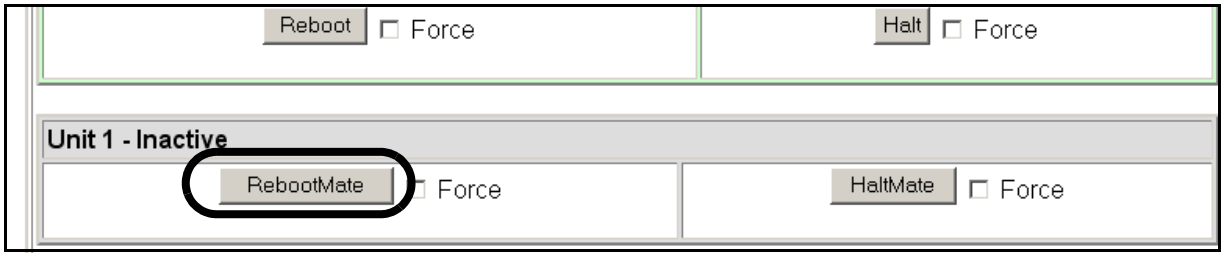
3 Review the status of the unit you want to reboot.



4 Click the **Reboot** button (for the active unit) or **RebootMate** button (for the inactive unit) for the Policy Controller unit you want to reboot.

Note 1: If you want to override any pre-reboot queries including a pre-checked by applications running on the unit, click the **Force** check box before clicking the **Reboot** or **RebootMate** button.

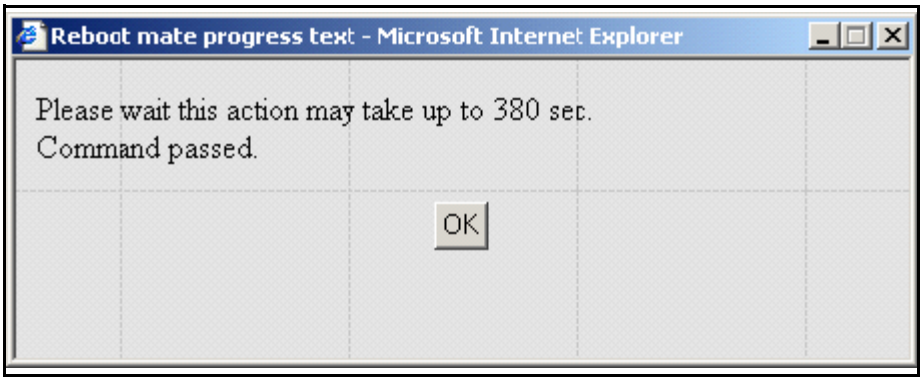
Note 2: In a system operating in fault-tolerant (duplex) mode, only the inactive unit can be rebooted using RebootMate or a Forced RebootMate. A Reboot or Forced Reboot can only be performed if the system is operating in simplex mode.



The system responds with the following message:

5 Click **OK** to confirm the reboot operation.

The NGCL and all call activity on the affected unit is shutdown and the unit begins to reboot. The system responds with the following message box:



6 Click **OK** to close the dialog box.

The NGCL and all call activity on the affected unit is shutdown.

Note 1: If you receive the following message, you must reboot the unit using the Alternate command line interface (CLI) method on page 77 otherwise consult section Troubleshooting reboots on page 77.

```
Error: Command failed. Reason: Mate not
available.
```

Note 2: If you try to reboot an active unit in duplex mode, you will receive the following message:

```
Error: Reboot - Command rejected. Reason:
Request only supported on INACTIVE unit when
system is in DUPLEX mode.
```

7 Use procedure View the operational status of a Policy Controller NCGL platform on page 43 to confirm the recovery of the unit after reboot.

8 This procedure is complete. If you were sent to this procedure by another procedure, return to that procedure and continue with the steps.

Troubleshooting reboots

The following possible error messages received during a reboot attempt and their meaning are described:

Error: Reboot - Command rejected. Reason: Mate is available.
The user has attempted to reboot the active server when the inactive server is available.

Error: Halt - Command rejected. Reason: Mate is available.
The user has attempted to halt the active server when the inactive server is available.

Error: Command failed. Reason: PRECHECK FAILED: application rejected request.
The user has attempted to rebootmate or haltmate command and the application rejected the request. The user should check /var/log/designlog to determine the name of the application that rejected the maintenance command.

Actions:

- Using the Force option overcomes a pre-check failure by any application running on the unit.
- Try the operation again later. If the problem persists, then contact Nortel Networks support personnel for assistance.

Alternate command line interface (CLI) method

ATTENTION
All prerequisites and limitations and restrictions shown on page 74 apply for this procedure.

At the Policy Controller console interface

1 Log onto the active Session Server unit and change to the root user.

2 Reboot the selected Session Server unit by typing

`# mtcli rebootmate` (to reboot the inactive unit)

or

`# mtcli reboot` (to reboot the active unit operating in simplex mode)

and pressing the **Enter** key.

3 Use procedure View the operational status of a Policy Controller NCGL platform on page 43 to confirm the recovery of the unit after reboot.

4 You have completed this procedure.

Acquire patch files

Purpose of this procedure

Use this procedure to identify patch files from a DVD-ROM or ESD archive file and copy them to the patch holding directory on each Policy Controller unit. This procedure may be used as a standalone task or as part of a higher level activity found in section Patching the NCGL platform on page 24 or Applying a maintenance release upgrade on page 2.

Limitations and Restrictions

As this is not a service impacting procedure, it can be performed on either the active or inactive units.

Prerequisites

If locating patch files from a DVD disk, ensure that the maintenance release or patching DVD-ROM disk is inserted into the unit DVD-ROM drive.

If reading release notes from an ESD delivered ISO archive file, ensure that the software archive file has been extracted and put into the /opt/swd directory on both units using procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 31.

Action

If locating patch files from a DVD disk, proceed with procedure Procedure: Acquire patch files from a DVD-ROM disk.

If locating patch files from an ESD delivered ISO maintenance release image file, then go to Procedure: Acquire patch files from an ESD delivered ISO image on page 81.

Procedure: Acquire patch files from a DVD-ROM disk

At a client workstation on the CS-LAN or IEMS client

1 Log onto the inactive Policy Controller unit using a secure shell by typing

> **`ssh -l <userid> <inactive_SS_IP_address>`**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

inactive_SS_IP_address
is the IP address of the inactive Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Insert the CD/DVD-ROM disk into the disk drive.

6 Mount the DVD-ROM drive by typing

```
$ mount /cdrom
```

and pressing the Enter key.

7 Change directories to the mounted DVD-ROM file system by typing

```
$ cd /cdrom
```

and pressing the Enter key.

8 Locate the patch files by typing

```
$ ls
```

and pressing the Enter key.

The system responds by displaying a list of files. Locate the patch files with the following filename format:

ncgl_samxts_patch_<rel#>.<wk#>.<major#>.<minor#>

Example
ncgl_samxts_patch_5.31.1.1

ncgl_samxts_patch_5.31.1.2

9 Copy the patch files from the CD/DVD-ROM disk to the patch holding directory on the Policy Controller unit by typing

```
$ cp <patchfilename> /patch/patchholding
```

and pressing the Enter key.

where

patchfilename
list the file name for the patch file

10 Change directories to root by typing

`$ cd /`

and pressing the Enter key.

11 Unmount the DVD-ROM drive by typing

`$ umount /cdrom`

and pressing the Enter key.

12 Repeat this procedure on the mate Policy Controller unit.

13 You have completed this procedure.

Procedure: Acquire patch files from an ESD delivered ISO image

At a client workstation on the CS-LAN or IEMS client

1 Log onto the inactive Policy Controller unit using a secure shell by typing

> **`ssh -l <userid> <inactive_SS_IP_address>`**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

inactive_SS_IP_address
is the IP address of the inactive Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

$ **`su - root`**

and pressing the Enter key.

4 When prompted, enter the root password.

5 Change directories to the directory where the maintenance release ISO image (and associated patch files) is located by typing

`$ cd /opt/swd/<ESD_ISO_directory>`

and pressing the Enter key.

where

<ESD_ISO_directory>
is the directory containing the version of the ISO image and associated patch files.

Note: There may be multiple directories containing different versions of ISO images.

6 Locate the patch files by typing

`$ ls`

and pressing the Enter key.

The system responds by displaying a list of files. Locate patch files with the following filename format:

ncgl_samxts_patch_<rel#>.<wk#>.<major#>.<minor#>

Example
ncgl_samxts_patch_5.31.1.1

ncgl_samxts_patch_5.31.1.2

7 Copy the patch files from the /opt/swd/<ESD_ISO_directory> to the patch holding directory by typing

`$ cp <patchfilename> /patch/patchholding`

and pressing the Enter key.

where

patchfilename
list the file name for the patch file

8 Repeat the previous step for additional patch files you need to install.

9 Repeat this procedure on the mate Policy Controller unit.

10 You have completed this procedure.

Query status of NCGL patches

Application

Use this procedure to review the status of patch files on a Policy Controller unit and to ensure that a patching file has been installed on both units in the node. This procedure may be used as a standalone task or as part of a higher level activity.

Two patch query methods are available:

- Displaying patch status information for all patches on page 83
- Displaying detailed information for a specific patch on page 84

Prerequisites

Patch files must first be copied to the Policy Controller unit.

Action

Displaying patch status information for all patches

At a client workstation on the CS-LAN or IEMS client

1 Open a secure shell to a Policy Controller unit by typing

> **ssh -l <userid> <SS_IP_address>**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

SS_IP_address
is the IP address of the selected Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

$ **su - root**

and pressing the Enter key.

4 When prompted, enter the root password.

5 To display patch status information for all patches type:

 # patch_ha -o QueryAll

and press the Enter key.

6 To compare this patch information to that on the mate unit, repeat this procedure for the second (mate) Policy Controller unit.

7 You have completed this procedure.

Displaying detailed information for a specific patch

At a client workstation on the CS-LAN or IEMS client

1 Open a secure shell to a Policy Controller unit by typing

> **ssh -l <userid> <SS_IP_address>**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

SS_IP_address
is the IP address of the Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

$ **su - root**

and pressing the Enter key.

4 When prompted, enter the root password.

5 To display detailed patch status information for a a specific patch on a unit, at the prompt type:

 # patch_ha -v <patch_version> -o QueryPatch

and press the Enter key.

where

patch_version
is the name of the patch file to be queried in the format: <NCGL_release_number>.<week_number>.<major_version_number>.<minor_version_number>

6 To compare this patch information to that on the mate unit, repeat this procedure for the second (mate) Policy Controller unit.

7 You have completed this procedure.

Apply and commit an NCGL patch

Purpose of this procedure

Use this procedure to apply patch files to the inactive Policy Controller unit. This procedure should only be used as part of the high level activity Apply and commit patches on page 28.

Restrictions and Limitations

ATTENTION
NCGL patch files should only be applied the inactive unit.

Patching activities must be completed on both units in the node.

Prerequisites

The patch files must have already been put into the **/patching/patchholding** directory on the Policy Controller hard drive. Contact your network administrator to determine if this has already been done. Refer to section Patching the NCGL platform on page 24 to copy patch file to the hard drives.

Action

At a client workstation on the CS-LAN or IEMS client

1 Log onto the inactive Policy Controller unit using a secure shell by typing

```
> ssh -l <userid> <inactive_SS_IP_address>
```

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

inactive_SS_IP_address
is the IP address of the Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Change directory to the patchholding directory by typing

$ **cd /patching/patchholding**

and pressing the Enter key.

6 Retrieve and untar the patch files from the patch archive to the /patching/<patch_version>/ directory, and fill the patching subsystem's database with the patch information. At the prompt, type:

 # patch_ha -f <patch_file_name> -o FetchPatch

and press the Enter key.

where

patch_file_name
is the name of the patch archive you want to extract patch files from

7 Validate the patch file to verify that the patch file is sane, and the patch is ready to be applied. At the prompt type:

 # patch_ha -v <patch_version> -o Validate

and press the Enter key.

where

patch_version
is the name of the patch file to be applied

8 Apply the patch file. Type:

 # patch_ha -v <patch_version> -o Apply

and press the Enter key.

where

patch_version
is the name of the patch file to be applied

ATTENTION

NCGL patches are not automatically committed when applied. In order for a patch to reapply the next time the unit is rebooted, it must first be committed.

9 Commit the patch so it is auto-applied at each reboot of the unit. Type:

patch_ha -v <patch_version> -o Commit

and press the Enter key.

where

patch_version
is the name of the patch file to be committed

10 If necessary, allow the unit to reboot or if requested, perform a reboot using procedure Reboot a Policy Controller unit on page 73. Otherwise skip to the next step.

11 Perform a status check of the unit including checking for newly generated logs and alarms, to ensure the inactive unit is operating without error. Refer to the Policy Controller Fault Management NTP, NN10438-911, for applicable procedures. If errors occur that are related to the patching activity, contact your next level of support.

Note: Checking unit status can entail different activities depending on what type of software item has been patched and any special patch application requirements. For example, some software subsystem processes may require a reboot before a patch can become active, while other subsystem processes restart with the new patched version once the patch application is complete.

12 You have completed this procedure. If you were forwarded to this procedure from another procedure, return to that procedure now and continue with the steps.

Remove an NCGL patch

Purpose of this procedure

Use this procedure to perform the following tasks:

- Remove patches from the inactive Policy Controller unit.
- Use this procedure only as part of the high level task Remove patches on page 29.

Restrictions and Limitations

ATTENTION
Remove NCGL patch files only from the inactive unit.

Patching activities must be completed on both units in the node.

Prerequisites

Verify which patches should be removed by referring to the patching or maintenance release notes.

Action

Remove an NCGL patch

At a client workstation on the CS-LAN or IEMS client

1 Log onto the inactive Policy Controller unit using a secure shell by typing

```
> ssh -l <userid> <SS_IP_address>
```

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

SS_IP_address
is the IP address or host name of the Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Uncommit the patch by typing:

patch_ha -v <patch_version> -o Uncommit

and pressing the Enter key.

where

patch_version
is the name of the patch file to be uncommitted

6 Remove the patch files and replace them with the files that existed prior to the patch. At the prompt type:

 # patch_ha -v <patch_version> -o Remove

and press the Enter key.

where

patch_version
is the name of the patch file to be removed

7 Delete the patch file. Type:

 # patch_ha -v <patch_version> -o Delete

and press the Enter key.

where

patch_version
is the name of the patch file to be deleted

8 If necessary, allow the unit to reboot or if requested, perform a reboot using procedure Reboot a Policy Controller unit on page 73.

9 This procedure is complete. Return to procedure Remove patches on page 29.

Upgrade/rollback/reinstall the Policy Controller application

Purpose of this procedure

Use this procedure to install the Policy Controller application onto a Policy Controller unit using one of the following methods:

- Reinstall a current version of the Policy Controller Application.
- Upgrade to a newer version of the Policy Controller Application (Maintenance Release).
- Rollback to a previous version of the Policy Controller Application.

ATTENTION

It is recommended that this procedure only be used as part of the high level activity Perform a maintenance release upgrade on page 8.

Limitations and restrictions

If the Policy Controller node is in operation and performing call processing activities, only perform this procedure on the standby unit.

Prerequisites

CAUTION

Use care when you perform this procedure. This procedure may cause the loss of customer data. Ensure that you have backed up the Policy Controller application database before performing this procedure by using procedure Perform a manual backup of the Policy Controller database on page 149.

Action

If reinstalling, upgrading or rolling back the Policy Controller application from an ESD delivered ISO image file, then go to Reinstall, upgrade or rollback the Policy Controller application from an ISO image file on page 96. Otherwise, continue with this procedure.

Reinstall, upgrade or rollback the Policy Controller application from a DVD-ROM disk

At the Policy Controller Serial Console

1 Log onto the inactive Policy Controller unit using a secure shell by typing

> **`ssh -l <userid> <inactive_SS_IP_address>`**

and press **Enter**.

where

userid
is a valid userid (like mtc) on the Policy Controller

inactive_SS_IP_address
is the IP address of the Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

```
$ su - root
```

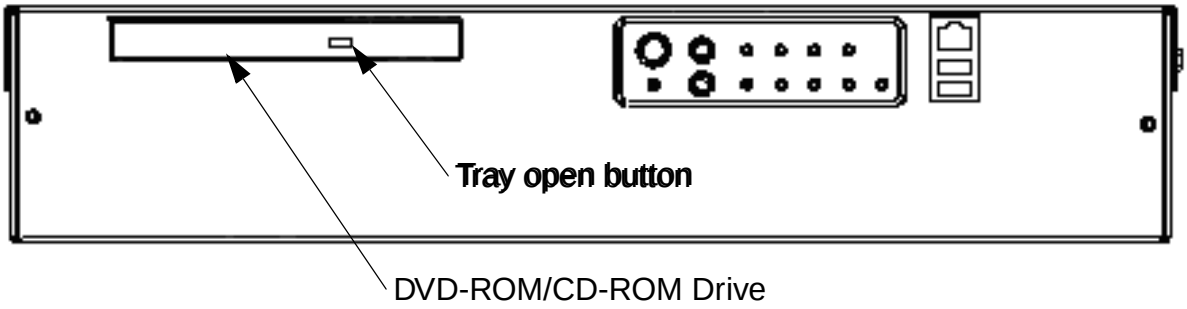
and press **Enter**.

4 When prompted, enter the root password.

5 Ensure that the DVD-ROM disk containing the Policy Controller Application is inserted before continuing.

Note: In some cases the Policy Controller Application may be on its own disk or it may be on the NCGL DVD data disk.

Policy Controller Front Panel



6 At the prompt, type

mount /cdrom

and press **Enter**.

The operating system may respond with the following warning:

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

7 From the root level, at the prompt, type

/cdrom/Tools/InstallApps <app>

Note: For **<app>**, type **spc** or **SPC**

and press **Enter**.

The operating system responds:

```
The Policy Controller Application layer is
currently installed. Do you wish to uninstall
the previous application and install the newer
version? (yes, no)
```

8 Type

yes

and press **Enter**.

The inactive unit begins installing the application. You will see messages scrolling on the screen.

After confirming the installation, the operating system responds and asks you for a tagname. For an upgrade, the tagname is already installed, but it can be changed.

```
-----------------------------------------------

- Get a tag name to allow Multiple HTTPS
connection through SSPFS -

-----------------------------------------------

Current tag name: prov

Do you wish to change the tag name (yes, no)
```

*If you do not want to change the tag name, type **no** and press **Enter.** If you want to change the tag name, type **yes,** enter the new tag name (The tag name cannot be **spc)**, and press **Enter**.*

9 After the application has completed installation, at the prompt, type

cd /

and press Enter.

10 Unmount the disk drive by typing

umount /cdrom

and pressing the Enter key.

11 Press the tray open button and remove the DVD-ROM disk from the drive.

12 You have completed this procedure. If applicable, return to Perform a maintenance release upgrade on page 8.

Reinstall, upgrade or rollback the Policy Controller application from an ISO image file

At the Policy Controller Serial Console

1 Log onto the inactive Policy Controller unit using a secure shell by typing

> **ssh -l <userid> <inactive_SS_IP_address>**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

inactive_SS_IP_address
is the IP address or host name of the Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Verify that the CD/DVD-ROM drive is not currently mounted to the /cdrom directory by typing

umount /cdrom

and pressing the Enter key.

6 At the prompt, type

mount -o loop /opt/swd/<ESD_ISO_directory>/<ESD_file_ISO> /cdrom

and press **Enter**.

where

ESD_file_ISO
is the name of the maintenance release ISO file

Example
mount -o loop /opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_MNCL.ISO. /cdrom

The operating system responds with the following warning:

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

7 From the root level, at the prompt, type

/cdrom/Tools/InstallApps <app>

Note: For **<app>**, type **spc** or **SPC**

and press **Enter**.

The operating system responds:

```
The Policy Controller Application layer is
currently installed. Do you wish to uninstall
the previous application and install the newer
version? (yes, no)
```

8 Type

yes

and press **Enter**.

The inactive unit begins installing the application. You will see messages scrolling on the screen.

After confirming the installation, the operating system responds and asks you for a tagname. For an upgrade, the tagname is already installed, but it can be changed.

```
-----------------------------------------------

- Get a tag name to allow Multiple HTTPS
connection through SSPFS -

-----------------------------------------------

Current tag name: prov

Do you wish to change the tag name (yes, no)
```

*If you do not want to change the tag name, type **no** and press **Enter.** If you want to change the tag name, type **yes,** enter the new tag name (The tag name cannot be **spc)**, and press **Enter**.*

9 After the application has completed installation, at the prompt, type

cd /

and press Enter.

10 Umount the ISO image by typing

umount -f /opt/swd/<ESD_ISO_directory>/<ESD_file_ISO>

and pressing Enter.

Example
mount -f
/opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_
MNCL.ISO

11 You have completed this procedure. If applicable, return to the high-level activity Perform a maintenance release upgrade on page 8.

Verify synchronization status of Policy Controller units

Purpose of this procedure

Use this procedure to determine the synchronization status of the Policy Controller units. Use this procedure as a standalone task or as part of a higher level activity.

Limitations and restrictions

There are no limitations or restrictions for this procedure.

Prerequisites

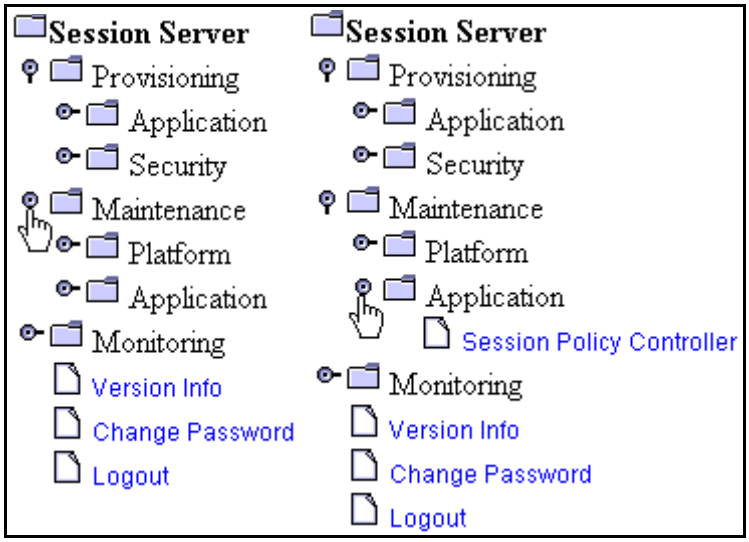
There are no prerequisites for this procedure.

Action

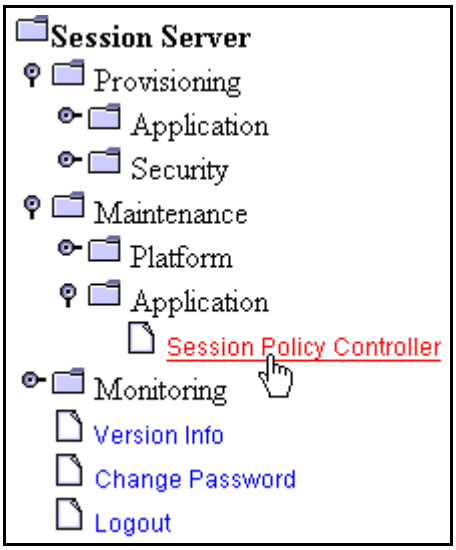
At the CS 2000 Session Server Launch Point

1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.

2 At the **Session Server** folder, click the **Maintenance folder,** then click the **Application** folder.

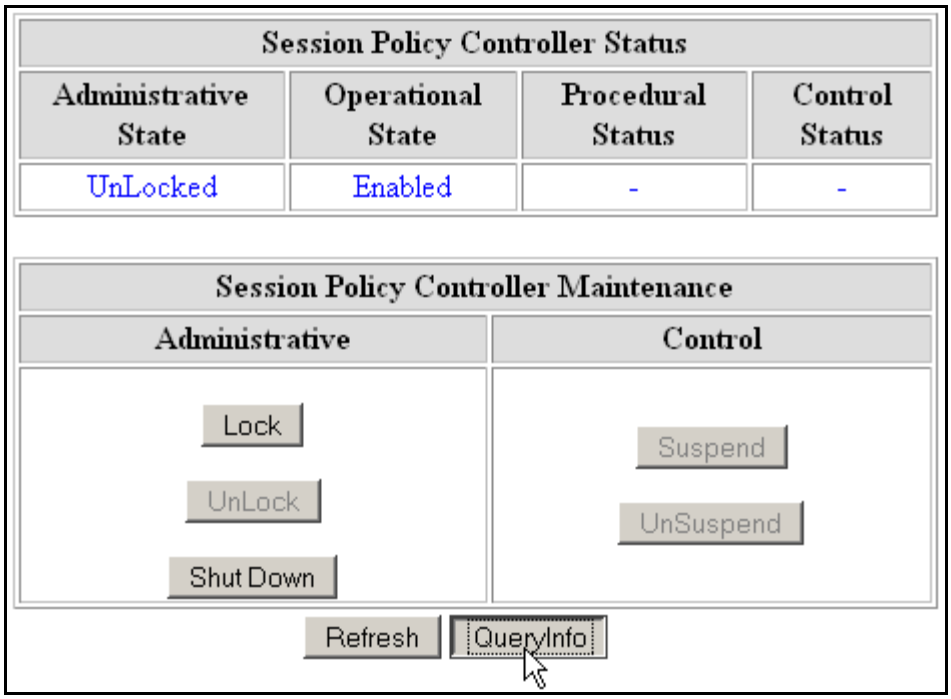


3 Click on the Session **Policy Controller** link.



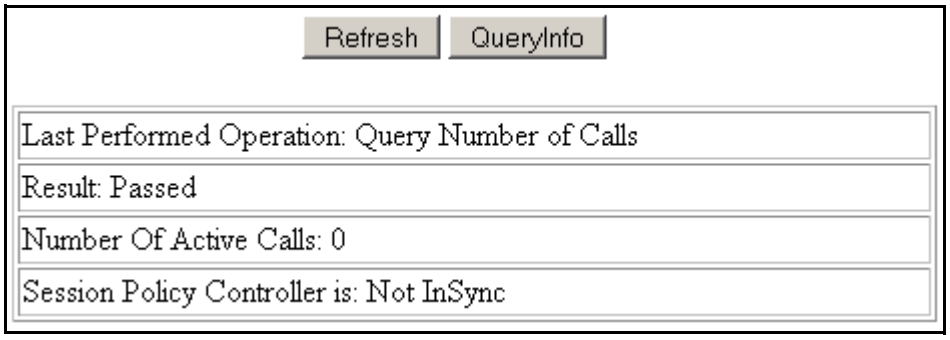
The **Policy Controller Maintenance** panel opens.

4 At the bottom of the **Policy Controller Maintenance** panel, locate and click the **QueryInfo** button.



5 The synchronization status of the Policy Controller units displays at the bottom of the query results panel.

If the units are not in sync, execute procedure *View Policy Controller alarms*, found in the Policy Controller Fault Management NTP, NN10438-911, and check for alarm conditions.



6 You have completed this procedure. If you were forwarded to this procedure by another procedure, return to that procedure and continue.

Invoke a maintenance SwAct of the Policy Controller platform

Purpose of this procedure

This procedure manually performs a maintenance SwAct (switch of activity) of the Policy Controller platform. A SwAct gracefully transitions call processing activity from the active Policy Controller unit to the standby unit without first reloading and reinitializing the Policy Controller application on the standby unit. All call data and Bandwidth resource usage counters for the Policy Application will be maintained during SwAct.

Use this procedure as a standalone task or as part of a maintenance or fault clearing activity like replacing a faulty standby unit or a high-level activity such as upgrading a standby unit.

Note: An automatic failover SwAct can be initiated by the platform NCGL in cases of critical faults on the active unit. For more information about conditions required for a SwAct, refer to section Understanding conditions for a SWACT found in the Policy Controller Security and Administration NTP, NN10434-611.

Limitations and Restrictions

ATTENTION
A maintenance SwAct should only be performed when both the active and standby units are operationally enabled and their databases are synchronized.

You cannot SwAct Policy Controller units if the active unit Jam state is *jammed*. If the unit Jam state is jammed, refer to procedure Enable a system SwAct (Unjam) on page 107 to unjam the unit.

ATTENTION
Logins to the Policy Controller do not survive a platform SwAct.

Prerequisites

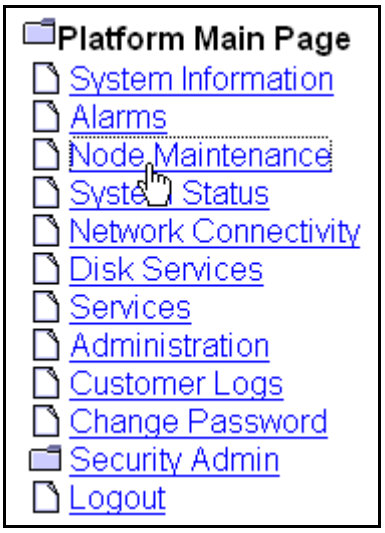
If you are executing a Forced SwAct, confirm that there are no alarm conditions.

Action

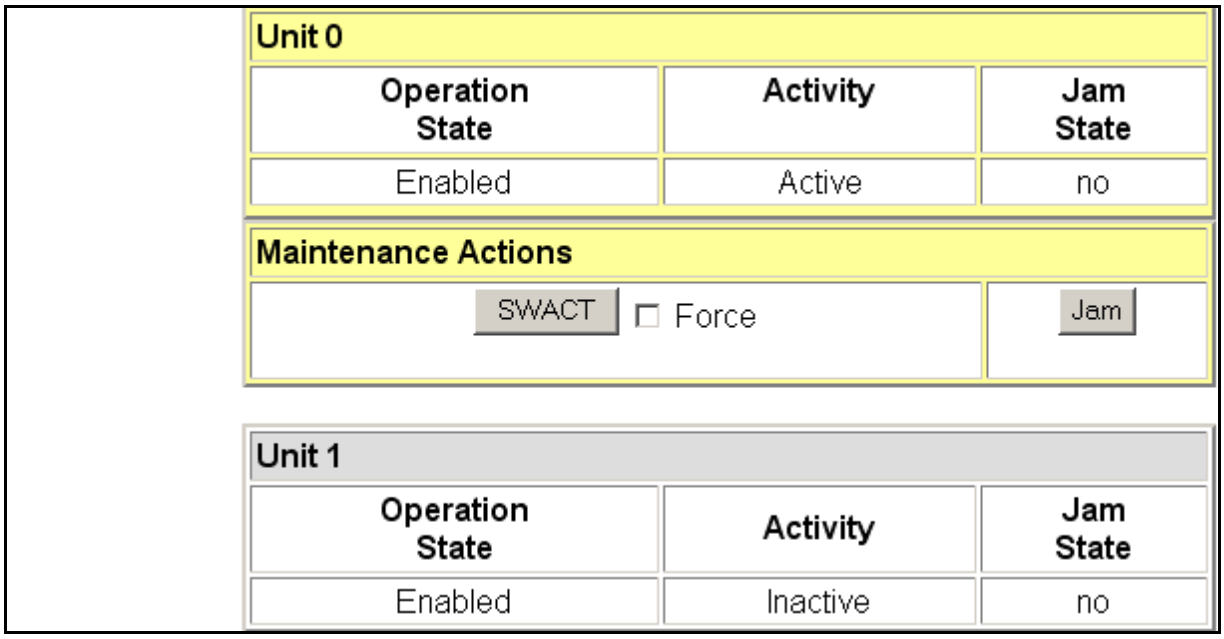
At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

2 Click the **Node Maintenance** link.



3 Refer to the table in section Additional status information on page 106 to review the description of the various fields of the Node Maintenance page.



4

CAUTION

Due to the risk for loss of data and service outage, it is recommended that the Forced SWACT option not be used except when instructed by your Nortel customer support representative.

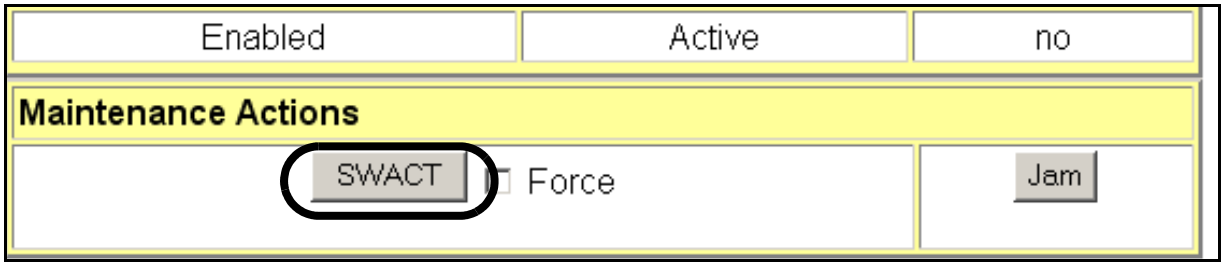
To SwAct the Policy Controller units, click the **SWACT** button.

OR

To override any pre-SwAct queries, first click the **Force** check box, then click the **SWACT** button.

Note: A forced SWACT overrides any SWACT pre-checks and is not recommended. SWACT pre-checks monitor the inactive unit for critical faults on the platform that should prevent a SWACT. In addition, the pre-check ensures that the Policy Controller application is in-sync. A SWACT force may result in a full service outage on the Policy Controller node if the inactive unit is not in-sync. There are also potential for

losses of provisioned data if a SWACT to an unstable unit is completed.



The system responds:

```
Are you sure you wish to swact? This may cause
a service interruption to applications running
on this server. Click OK to confirm server swact
or cancel to abort.
```

5 Click **Yes** to confirm either the SwAct or forced SwAct.

6 Observe the *Activity* field for each unit. Each unit's activity status (whether Active or Inactive) swaps.

7 The procedure is complete. If applicable, return to procedure Perform a maintenance release upgrade on page 8.

Additional status information

The following table describes the various fields of the Node Maintenance panel.

Field	Description
Operation State (unit 0 or 1)	The operational state of the platform software, either enabled or disabled.
Activity (unit 0 or 1)	The activity state of the platform software, either active or inactive.
Jam State (active unit only)	Indicates whether or not the unit has been "jammed", preventing the standby unit from being able to become active, regardless of any failures on the active unit. States are either jammed, where a SwAct is disabled, or unjammed, where a SwAct is enabled.
Maintenance Actions (active unit only)	Maintenance panel for performing node SWACT activity and to jam or unjam node activity switches.

Enable a system SwAct (Unjam)

Purpose of this procedure

Use the Unjam command to manually enable a SwAct (switch of activity) of the active and stand-by units by allowing the two units to toggle their operational states.

Limitations and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as replacing a faulty standby unit or upgrading a standby unit.

Prerequisites

There are no prerequisites for performing this procedure.

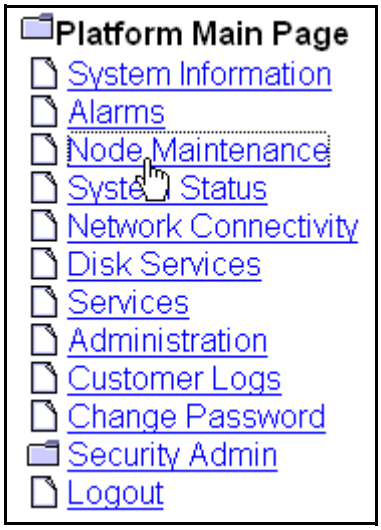
Action

Enable a system SwAct (Unjam)

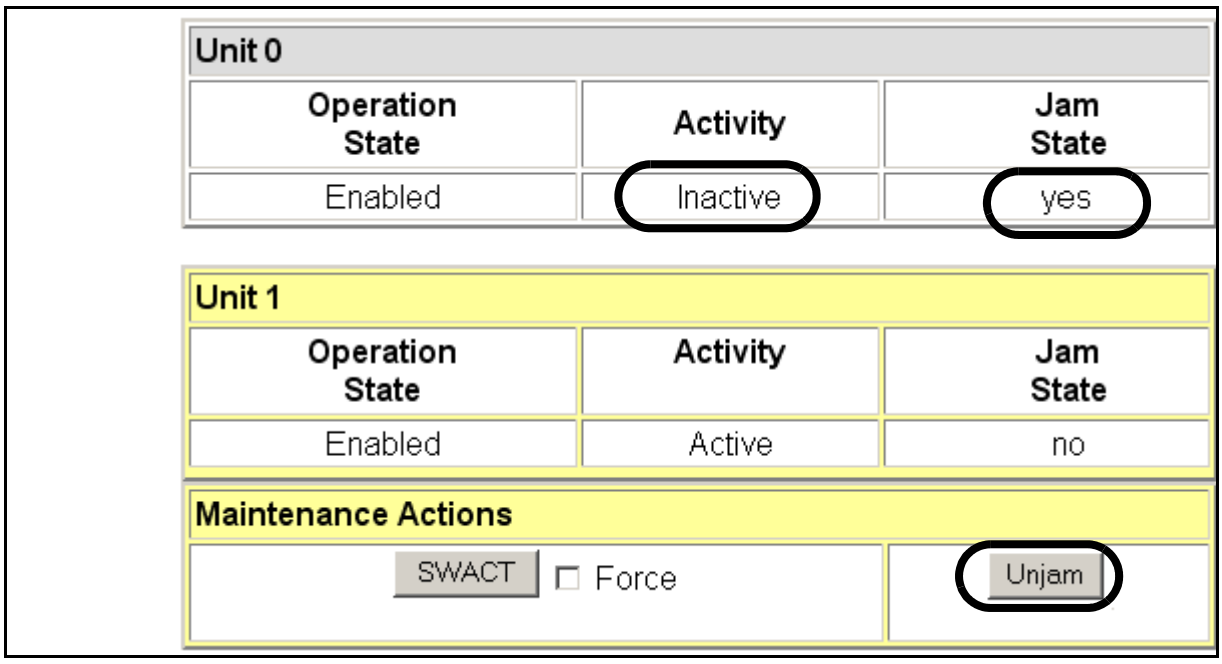
At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

2 Click the **Node Maintenance** link.



3 Determine if the Jam State of the standby unit is **Yes** or **No**. If it is **No**, then the unit is already unjammed and you are done with this procedure. If it is **Yes**, then continue with step 4.

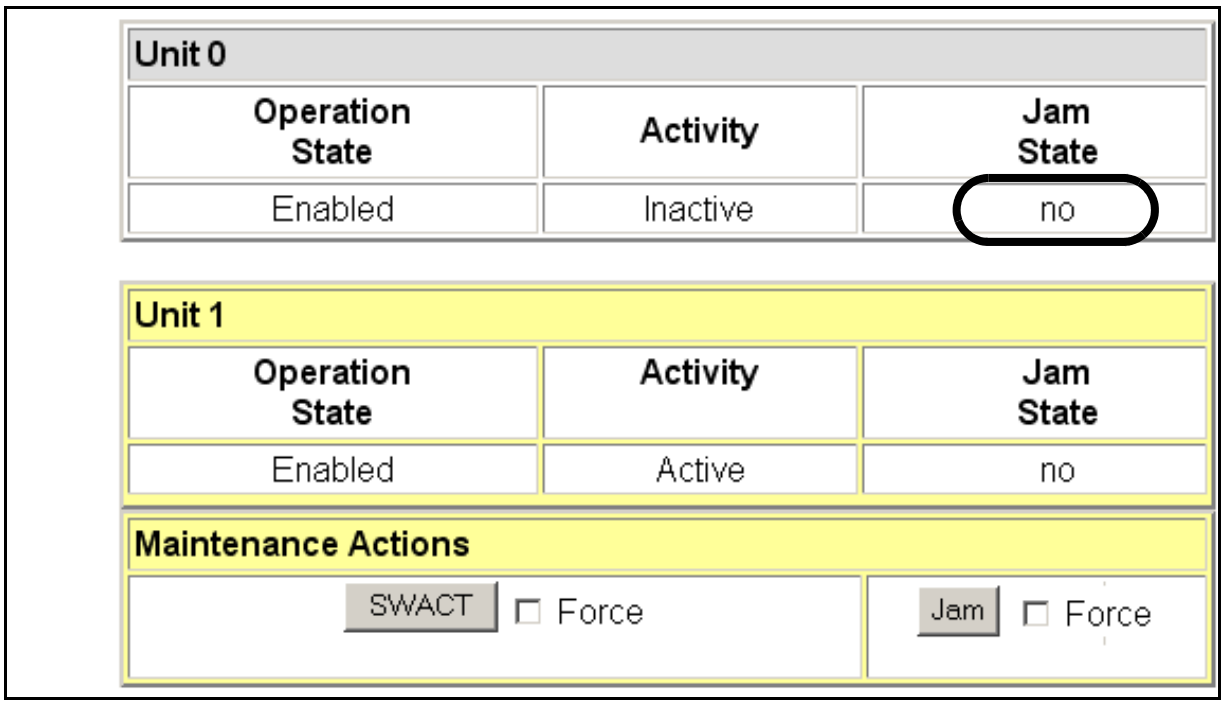


4 Click the **UnJam** button.

The system responds:

```
Info: Unjam - Command passed.
```

5 Observe the Jam state for the standby Policy Controller unit transitions from **Yes** to **No**.



Unit 0		
Operation State	**Activity**	**Jam State**
Enabled	Inactive	no

Unit 1		
Operation State	**Activity**	**Jam State**
Enabled	Active	no

Maintenance Actions	
SWACT ☐ Force	Jam ☐ Force

6 You have completed this procedure. If applicable, return to Perform a maintenance release upgrade on page 8.

Rollback a Policy Controller NCGL platform software upgrade

Purpose of this procedure

This procedure describes how to use the NCGL Platform Manager software to rollback a maintenance release NCGL platform.

ATTENTION

Only use this procedure as part of the high level activities Abort a maintenance release upgrade on page 16 or Perform an emergency maintenance release rollback on page 19.

Limitations and Restrictions

You can only rollback to a previous load if it exists on the Policy Controller unit disk drive. If not, you must reinstall the load onto the disk drive from DVD-ROM disk or ESD ISO image. Refer to section Upgrade preparation on page 7 for instructions to perform this activity.

Prerequisites

ATTENTION

This procedure assumes that you are experiencing problems with a maintenance release upgrade on a single Policy Controller unit and that you have not upgraded the second unit in the node with the maintenance release. If you have already upgraded both units with the maintenance release and are having problems, then refer first to section Perform an emergency maintenance release rollback on page 19 for the complete prerequisite steps.

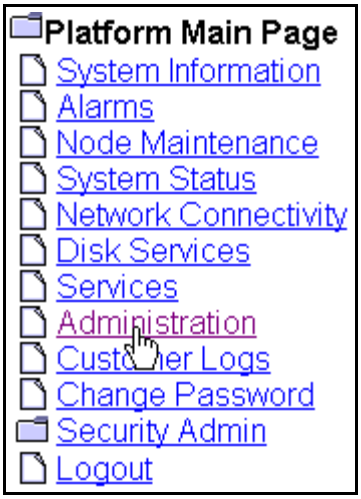
Action

At the CS 2000 Session Server Launch Point

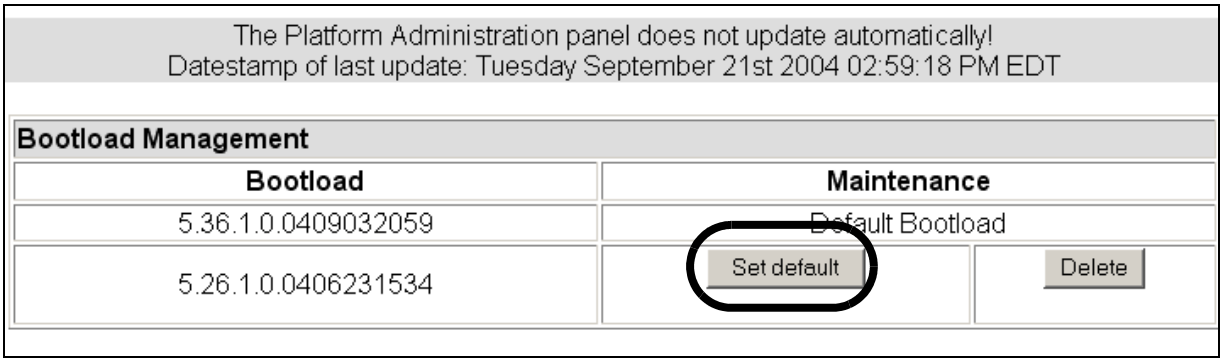
1 Select **Succession Communication Server 2000 NCGL Platform Manager** from the launch point menu.

The Platform Main Page menu is displayed.

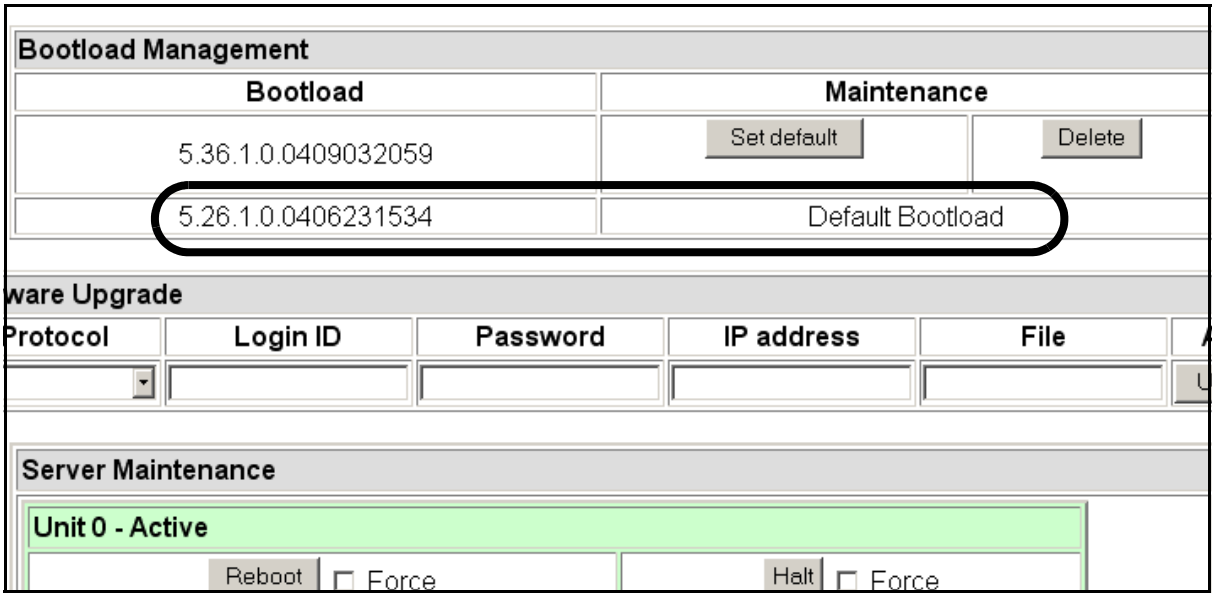
2 Click the **Administration** link.



3 Select the bootload version that you want to roll the NCGL platform back to and click the **Set default** button.



4 Verify that the default bootload has been set to the version previous to the maintenance release upgrade.



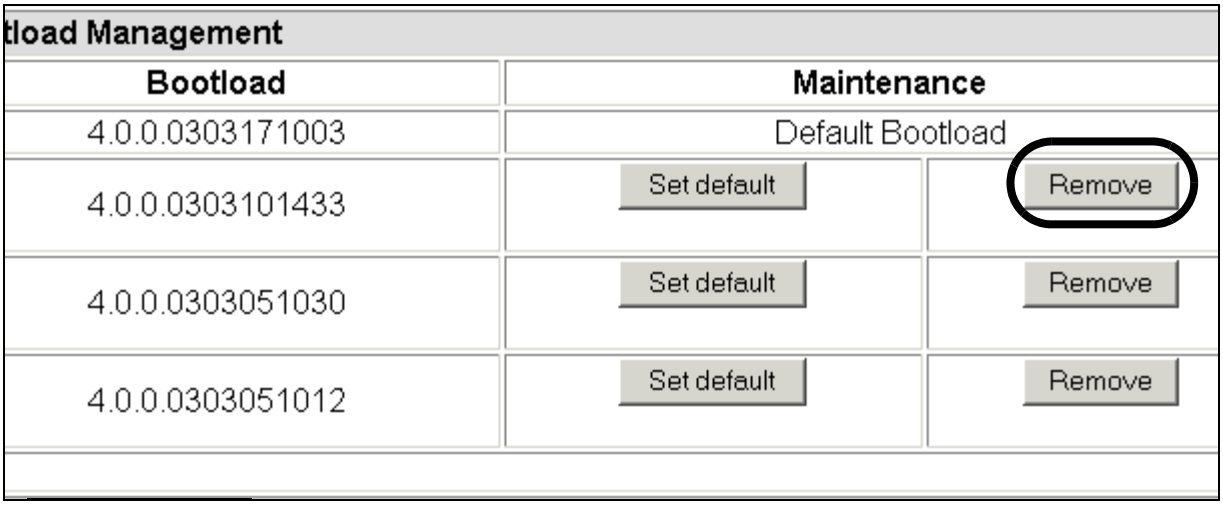
5 You have completed this procedure. Return to your applicable high-level activity: Abort a maintenance release upgrade on page 16 or Perform an emergency maintenance release rollback on page 19.

Additional information

By default, the Policy Controller units retain previous bootloads. For housekeeping purposes, older bootload versions may be manually removed by clicking the **Remove** button.

Note: You cannot delete the bootload that is set to be the default bootload, nor can you delete the currently running bootload.

If a bootload image upgrade is requested and insufficient disk space is available in the `/boot` directory, the NCGL software deletes the oldest bootload from the `/boot` directory and performs the requested bootload image upgrade. The system can not delete a bootload that is set to be the default bootload.



Drop database synchronization for the Policy Controller application

Purpose of this procedure

Use this procedure to drop call processing application and application database synchronization between the active and inactive Policy Controller units.

ATTENTION

Only use this procedure as part of the high level activity Perform an emergency maintenance release rollback on page 19.

Limitations and restrictions

Perform this procedure only on the active Policy Controller unit.

After this procedure has executed, the Policy Controller application database continues in a non-synchronized state until a SwAct is performed.

CAUTION

Use care when you use this procedure as this procedure may cause the loss of customer data. Ensure that you have backed up the Policy Controller application database on the active unit before executing this procedure.

Prerequisites

There are no prerequisites for performing this procedure.

Action

If	Then
you are performing this procedure from a DVD-ROM disk	go to procedure Run dropSync script from a DVD-ROM disk on page 116.
you are performing this procedure from an ESD delivered ISO image file	go to procedure Run dropSync script from an ISO image file on page 117.

Run dropSync script from a DVD-ROM disk

At the Policy Controller Serial Console

1 Log onto the active Policy Controller unit using a secure shell by typing

```
> ssh -l <userid> <active_SS_IP_address>
```

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

active_SS_IP_address
is the IP address of the active Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

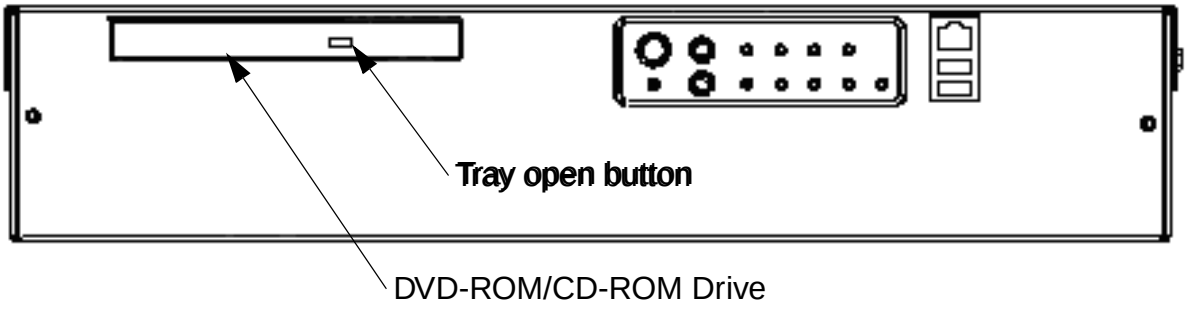
```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Ensure that the latest version of the software installation DVD-ROM disk is inserted into the active unit before continuing.

Policy Controller Front Panel



6 At the prompt, type

mount /cdrom

and press Enter.

The operating system responds with the following warning:

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

7 From the root level, at the prompt, type

./**cdrom/Tools/dropSync**

and press Enter.

8 After you are returned to the prompt, type

cd /

and press Enter.

9 Unmount the disk drive by typing

umount /cdrom

and pressing the Enter key.

10 If desired, press the tray open button and remove the DVD-ROM disk from the drive.

11 You have completed this procedure. Return to the high-level activity Perform an emergency maintenance release rollback on page 19.

Run dropSync script from an ISO image file

At the Policy Controller Serial Console

1 Log onto the active Policy Controller unit using a secure shell by typing

> **ssh -l <userid> <active_SS_IP_address>**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

active_SS_IP_address
is the IP address of the active Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

$ **su - root**

and pressing the Enter key.

4 When prompted, enter the root password.

5 Verify that the CD/DVD-ROM drive on the active unit is not currently mounted to the /cdrom directory by typing

umount /cdrom

and pressing the Enter key.

6 At the prompt, type

mount -o loop /opt/swd/<ESD_ISO_directory>/<ESD_file_ISO> /cdrom

and press **Enter**.

where

ESD_file_ISO
is the name of the maintenance release ISO file

Example
mount -o loop /opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_MNCL.ISO. /cdrom

The operating system responds with the following warning:

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

7 From the root level, at the prompt, type

./**cdrom/Tools/dropSync**

and press **Enter**.

8 After the application has completed installation, at the prompt, type

cd /

and press Enter.

9 Umount the ISO image by typing

umount -f /opt/swd/<ESD_ISO_directory>/<ESD_file_ISO>

and pressing Enter.

Example
mount -f /opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_MNCL.ISO

10 You have completed this procedure. Return to the high-level activity Perform an emergency maintenance release rollback on page 19.

Suspend the Policy Controller application

Purpose of this procedure

Use this procedure to temporarily take the Policy Controller application out of service.

Note: For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section of the Policy Controller Security and Administration NTP, NN10434-611.

Limitations and restrictions

This procedure can only be performed when the Policy Controller application is in the following service states:

- the Operational State is **Enabled**
- the Administrative State is **Locked**

Prerequisites

The Policy Controller application must have previously been locked. If it is not locked or you are uncertain of the state of the application, refer to procedure Lock the Policy Controller application on page 123.

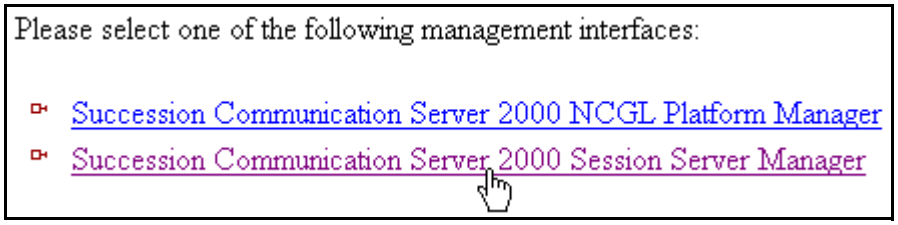
Action

CAUTION

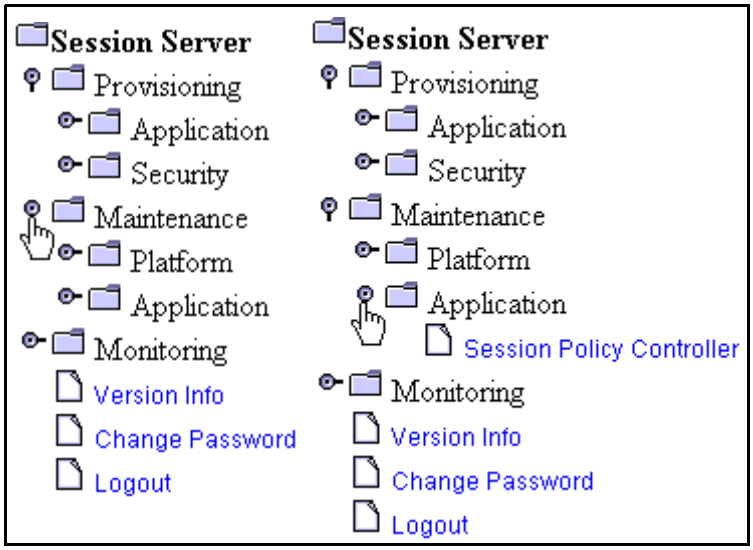
This procedure is used to temporarily take the Policy Controller out of service. Suspending the Policy Controller Application means the lines or gateways configured for Network Virtual Call Admission Control will be processed by the CS 2000 without the Virtual Call Admission Control function. When the Policy Controller is suspended, it is equivalent to being unreachable by the CS2000, but the Lines or Gateways will be able to continue to make or receive calls without the Policy Controller.

At the CS 2000 Session Server Launch Point

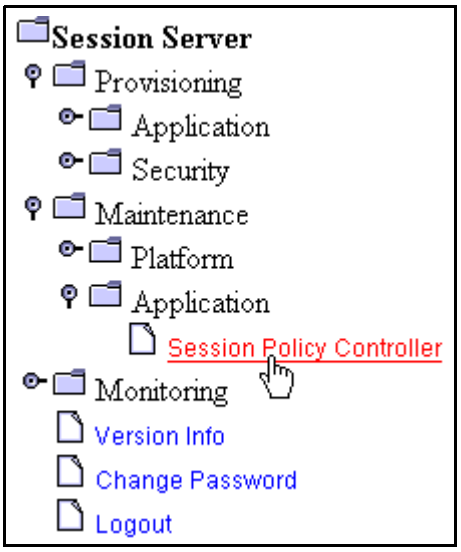
1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.



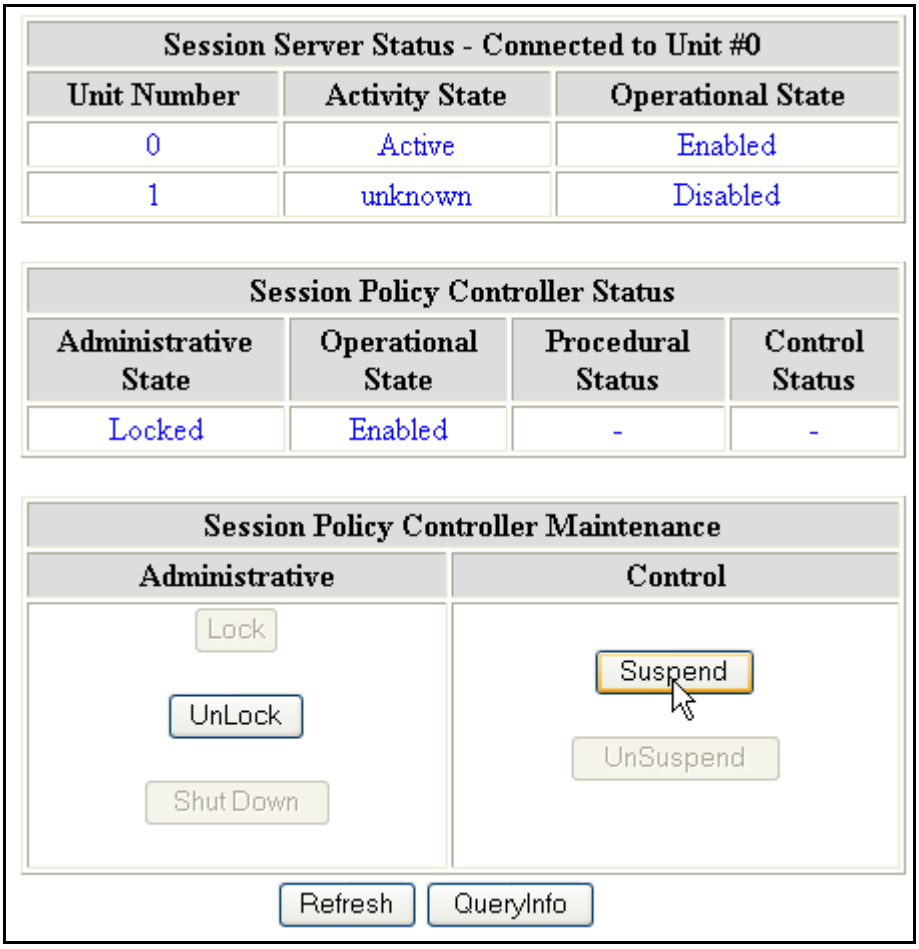
2 At the Session Server folder, click the **Maintenance folder,** then click the **Application** folder.



3 Click the **Session Policy Controller** link to open it.

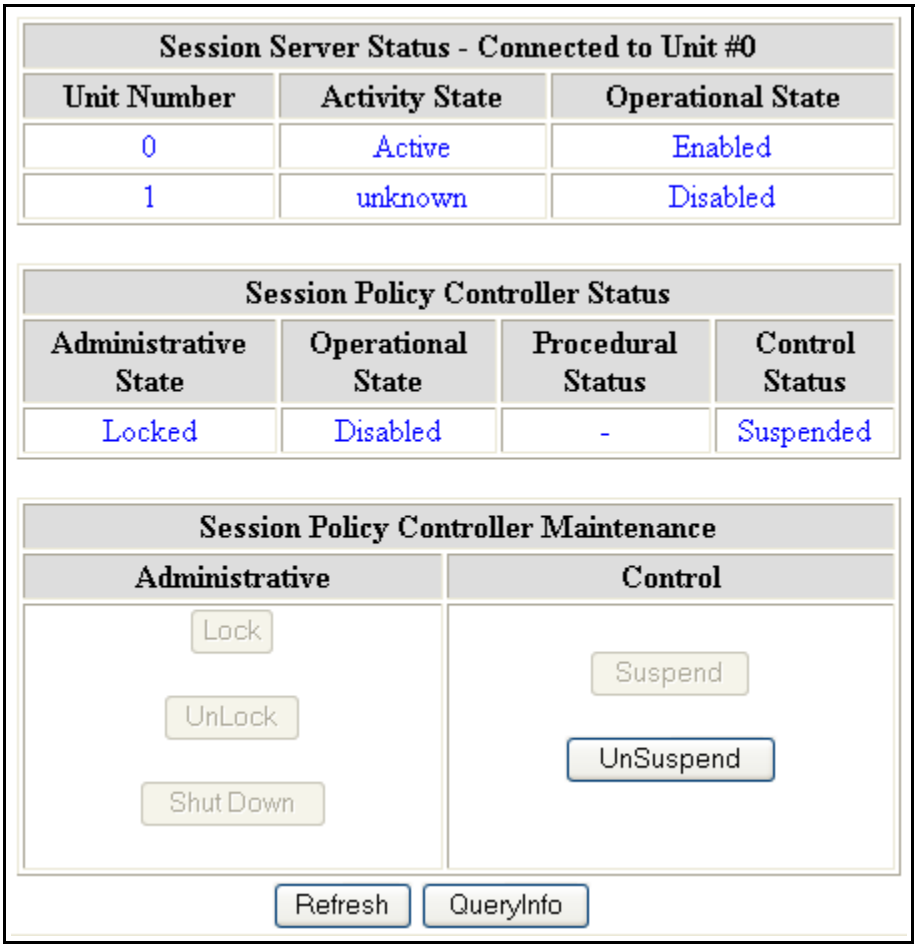


4 In the Policy Controller Maintenance panel click **Suspend**.



5 Monitor the status of the Policy Controller application in the Policy Controller Status box:

- the Operational State changes to **Disabled**
- the Control Status changes to **Suspended**



6 If applicable, restart the Policy Controller application by executing procedure Unlock the Policy Controller application on page 145.

7 The procedure is complete.

Lock the Policy Controller application

Purpose of this procedure

Use the following procedure to change the administrative status of the Policy Controller application to Locked. This will cause all call data to be reset, and will also automatically reset Bandwidth resource usage counters to zero for the Policy Controller.

Note: For more detailed information about Policy Controller application services states and administrative functions, refer to NTP *Policy Controller Security and Administration*, NN10434-611.

Limitations and restrictions

CAUTION

This is a service affecting procedure. Locking the Policy Controller application prevents any lines configured for Virtual Call Admission Control via the Policy Controller to make or receive calls. Existing calls regardless of call state will not be released by this procedure. However, once locked, the Policy Controller application will not be able to process any new VCAC requests.

Note: The CS 2000 will still process calls without Network VCAC if it determines the Policy Controller is in Locked State.

This procedure provides instructions for changing the service status of the Policy Controller application software only. For instructions on determining the status of the Policy Controller platform, refer to procedure View the operational status of a Policy Controller NCGL platform on page 43

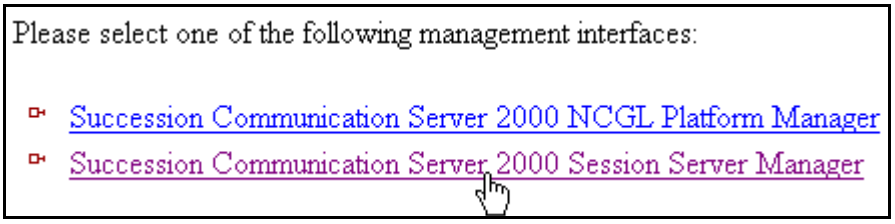
Prerequisites

There are no prerequisites for this procedure.

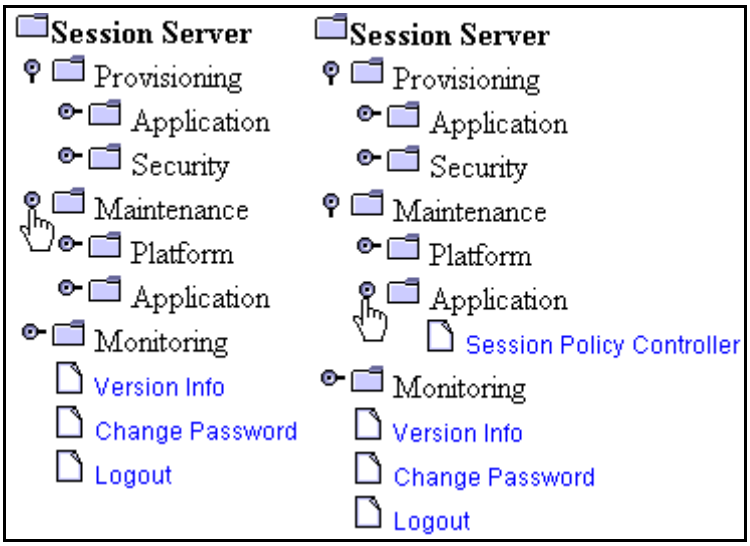
Action

At the CS 2000 Session Server Launch Point

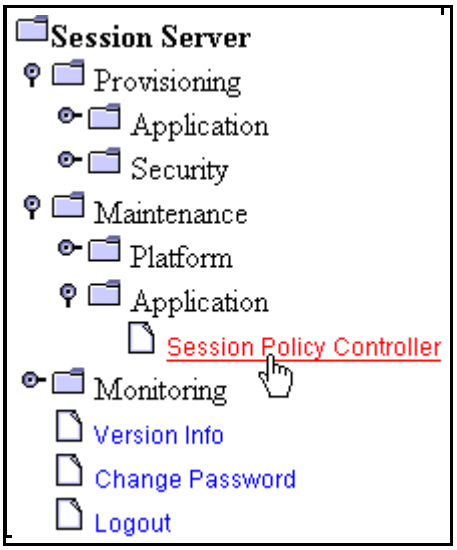
1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.



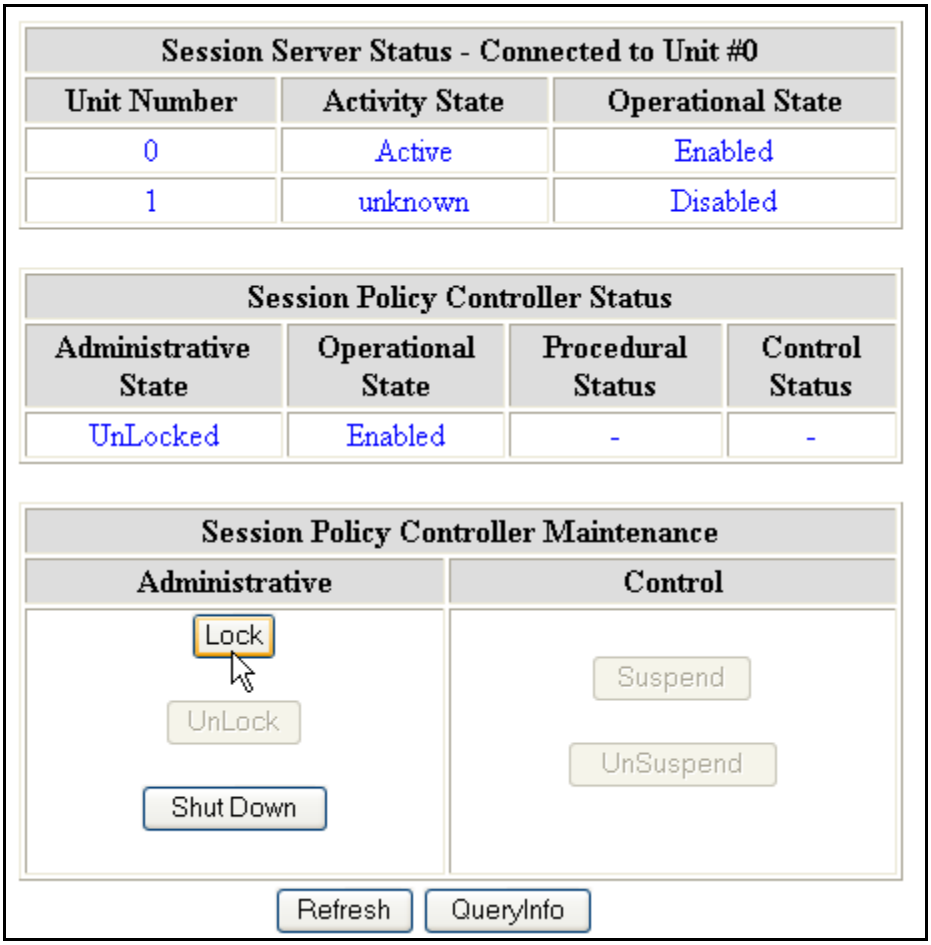
2 At the Session Server folder, click the **Maintenance folder**, then click the **Application** folder.



3 Click on the **Session Policy Controller** link to open it.



4 In the Policy Controller Maintenance panel click the **Lock** button.



The system responds with the following message box:

```
This action will release all existing Session
Policy Controller calls and will cause a SERVICE
OUTAGE on this Session Server. There are x
active calls. Do you wish to continue?
```

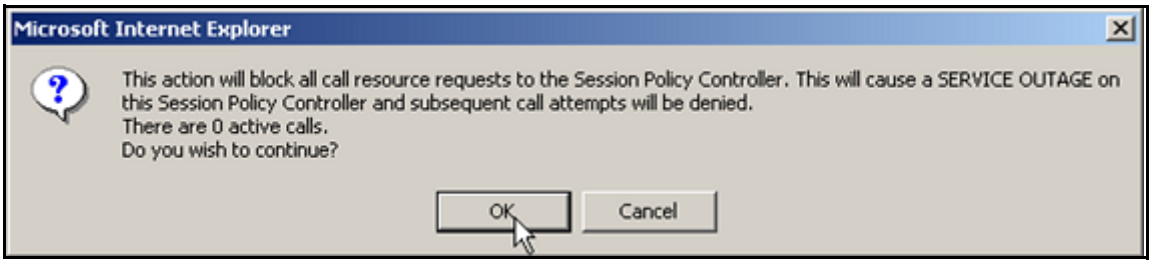
5

CAUTION

This is a service affecting procedure. Locking the Policy Controller application prevents any lines configured for Virtual Call Admission Control via the Policy Controller to make or receive calls. Existing calls regardless of call state will not be released by this procedure. However, once locked, the Policy Controller application will not be able to process any new VCAC requests.

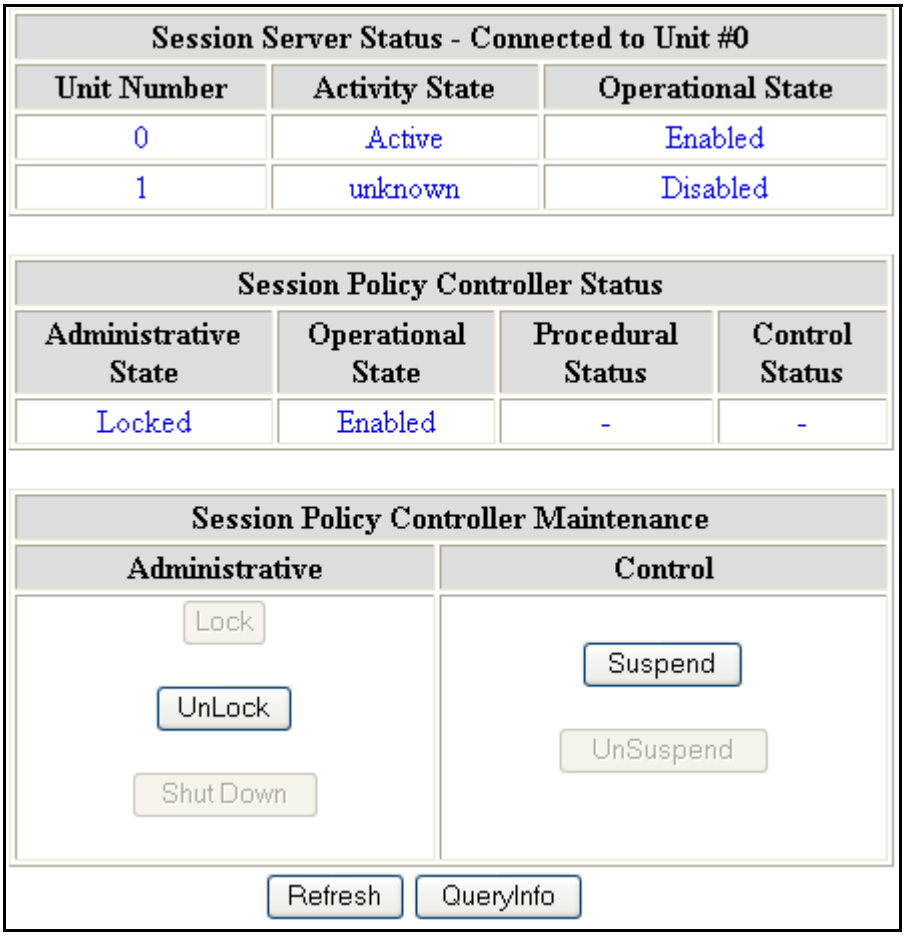
Note: The CS 2000 will still process calls without Network VCAC if it determines the Policy Controller is in Locked State.

Click **OK** to confirm locking the Policy Controller application or click **Cancel** to cancel the action and close the message box.

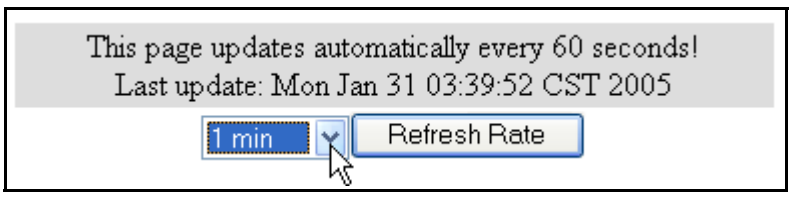


6 Monitor the status of the Policy Controller application in the Policy Controller Status box:

- the Administrative State changes to **Locked**



The status panel refreshes automatically according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the **Refresh Rate** button. Otherwise, manually refresh the panel by clicking on the **Refresh** button on the **Session Policy Controller Maintenance** panel.



7 You have completed this procedure.

View the operational status of the Policy Controller application

Purpose of this procedure

Use the following procedure to view the service status of the Policy Controller application. This procedure may be used as a standalone task or as part of a high-level activity.

Limitations and restrictions

This procedure provides instructions for determining the service status of the Policy Controller application software only. For instructions on determining the status of the Policy Controller platform, refer to procedure View the operational status of a Policy Controller NCGL platform on page 43.

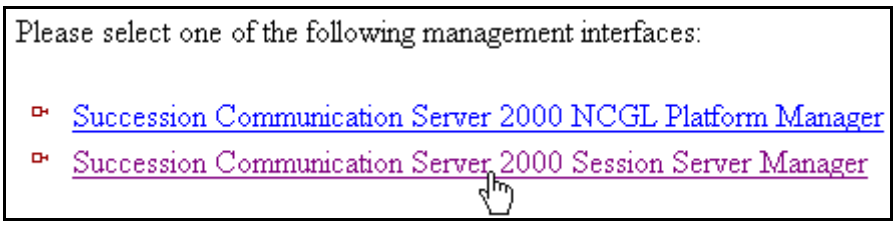
Prerequisites

There are no prerequisites for this procedure.

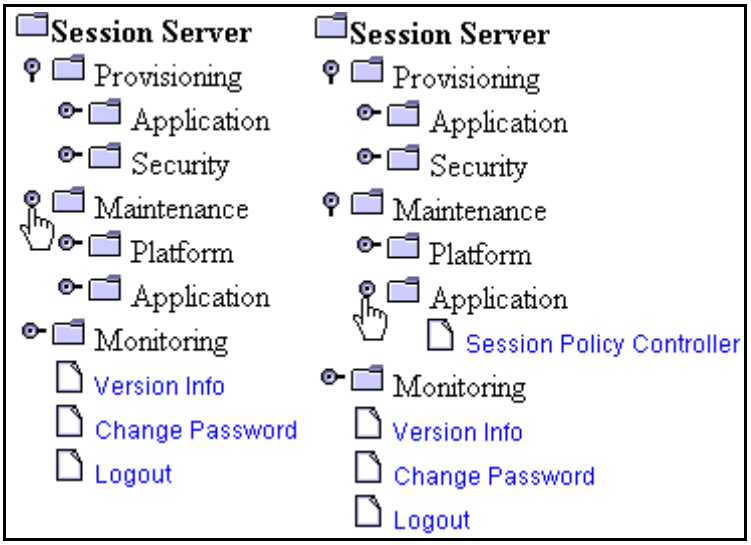
Action

At the CS 2000 Session Server Launch Point

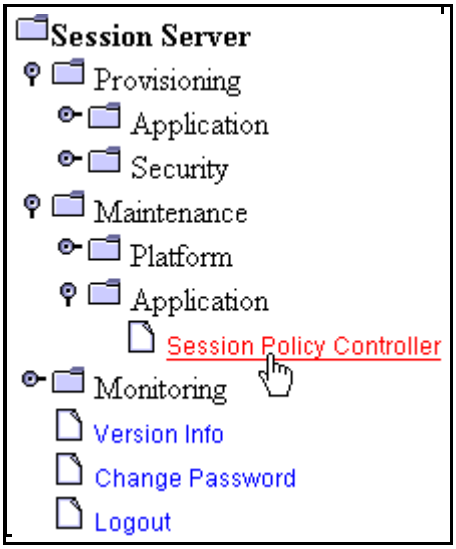
1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.



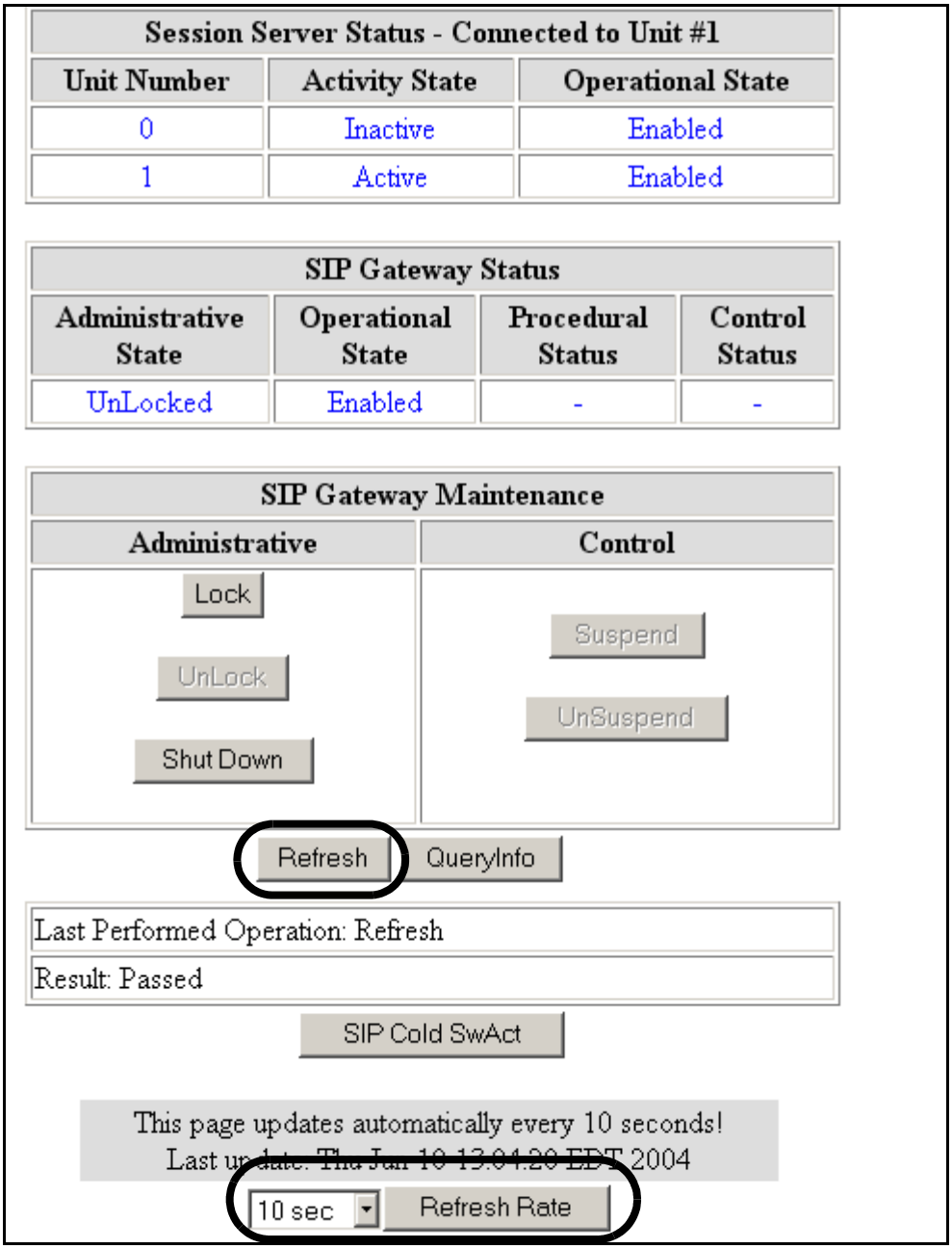
2 At the **Session Server** folder, click the **Maintenance folder,** then click the **Application** folder.



3 Click on the **Policy Controller** folder to open it.



4 Monitor the status of the Policy Controller application on the active Policy Controller node from this view.



Note: This view is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the **Refresh Rate** button or manually refresh the page by clicking the **Refresh** button.

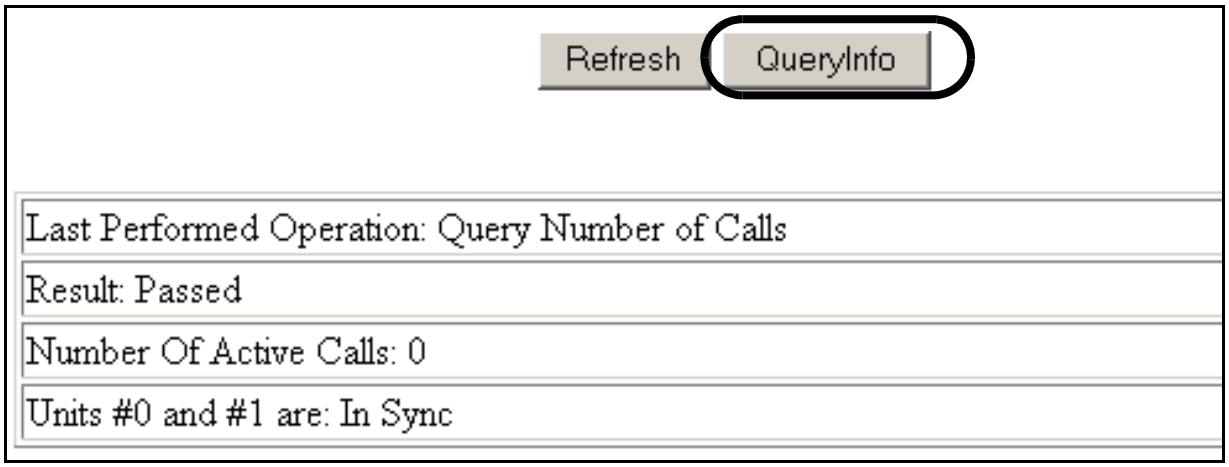
5 Refer to section Interpreting Policy Controller application status and maintenance fields on page 133 to review the description of the various fields of this view.

Note: For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section *Interpreting Policy Controller application states* found in the Policy Controller Security and Administration NTP, NN10434-611.

6 To perform available Policy Controller application maintenance activities, refer to the following procedures found in the Policy Controller Security and Administration NTP, NN10434-611:

- Lock the Policy Controller application
- Unlock the Policy Controller application
- Suspend the Policy Controller application
- Unsuspend the Policy Controller application
- Shutdown the Policy Controller application
- Cold SwAct the Policy Controller application

7 To view the number of active calls currently being handled by the application and the sync status of the Policy Controller units, click the **QueryInfo** button.



8 You have completed this procedure.

Interpreting Policy Controller application status and maintenance fields

Use the following table to assist you in interpreting the Policy Controller Status area.

Policy Controller node status field descriptions

Field	Description
Unit Connection Status Bar	Indicates which Policy Controller unit in the node the CS 2000 Policy Controller Manager is connected to.
Unit Number	indicates the units in the Policy Controller node, (labelled 0 and 1) and a maximum of one node on the Call Server-LAN
Activity State	indicates which unit is Active and which is Inactive (standby), also an indirect indicator of fault-tolerant status, assuming both units are operational.
Operational State	indicates the service status of each Policy Controller unit (either Enabled or Disabled).

Use the following table to assist you in interpreting the Policy Controller status area.

Policy Controller application Status field descriptions

Field	indication
Administrative State	Locked, Unlocked, ShuttingDown
Operational State	Enabled or Disabled
Procedural Status	Terminating or -
Control Status	Suspended or -

Use the following table to assist you in interpreting the Policy Controller area's CCITT X.731-style and related DMS-style status indicators:

Policy Controller Maintenance field descriptions and interpretation of service states

Administrative State	Operational State	Procedural Status	Control Status	DMS style Service States
Locked	Disabled	-	Suspended	Offline (OFFL)
Locked	Enabled	-	-	Manual Busy MANB)
Locked	Enabled	Terminating	-	Manual Busy Transitioning (MANBP)
Unlocked	Enabled	-	-	In Service (INSV)
Unlocked	Disabled	-	-	System Busy (SYSB)
Shutting Down	Enabled	-	-	Going out of service (INSVD)

Note: (-) indicates a status of in-service

Unsuspend the Policy Controller application

Purpose of this procedure

Use the following procedure to bring the Policy Controller application back into service without restarting the Policy Controller application.

Note: For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section “Interpreting Policy Controller application states” in the Policy Controller Security and Administration NTP, NN10434-611.

Limitations and restrictions

This procedure can only be performed when the Policy Controller application is in the following service states:

- the Operational State is **Disabled**
- the Administrative State is **Locked**
- the Control Status is **Suspended**

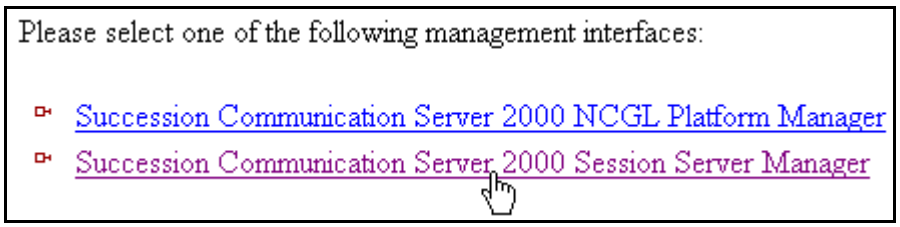
Prerequisites

The Policy Controller application must previously have been suspended. If it is not suspended or you are uncertain of the state of the application, refer to procedure Suspend the Policy Controller application on page 119.

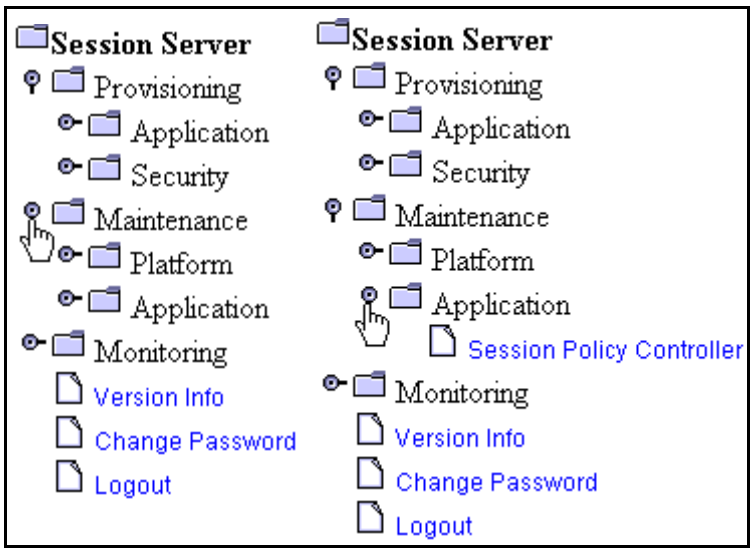
Action

At the CS 2000 Session Server Launch Point

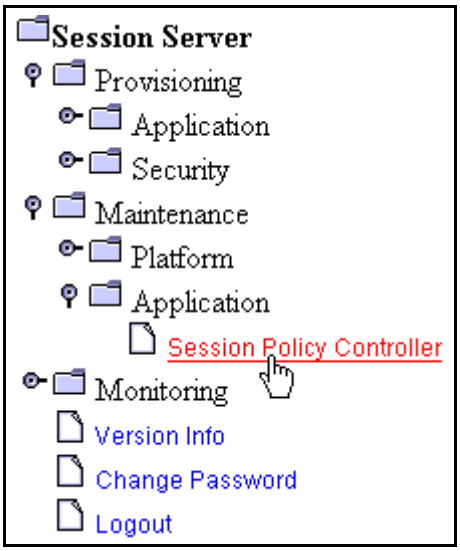
1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.



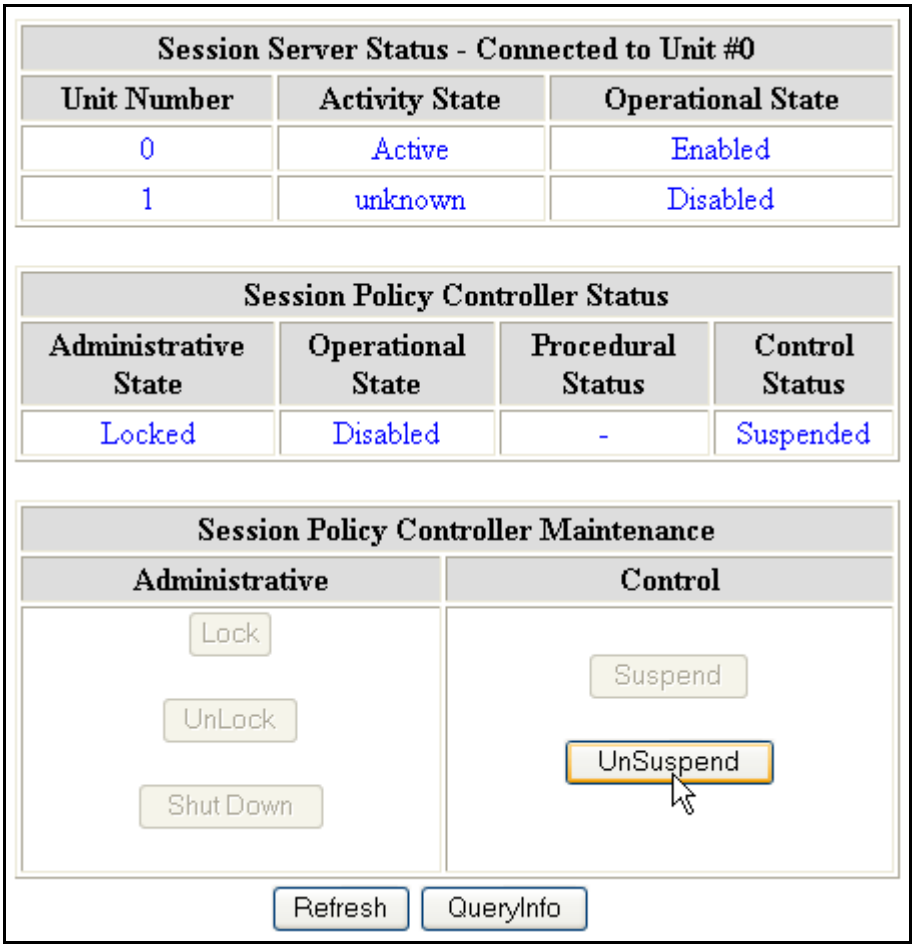
2 At the **Session Server** folder, click the **Maintenance folder,** then click the **Application** folder.



3 Click on the **Policy Controller** folder to open it.

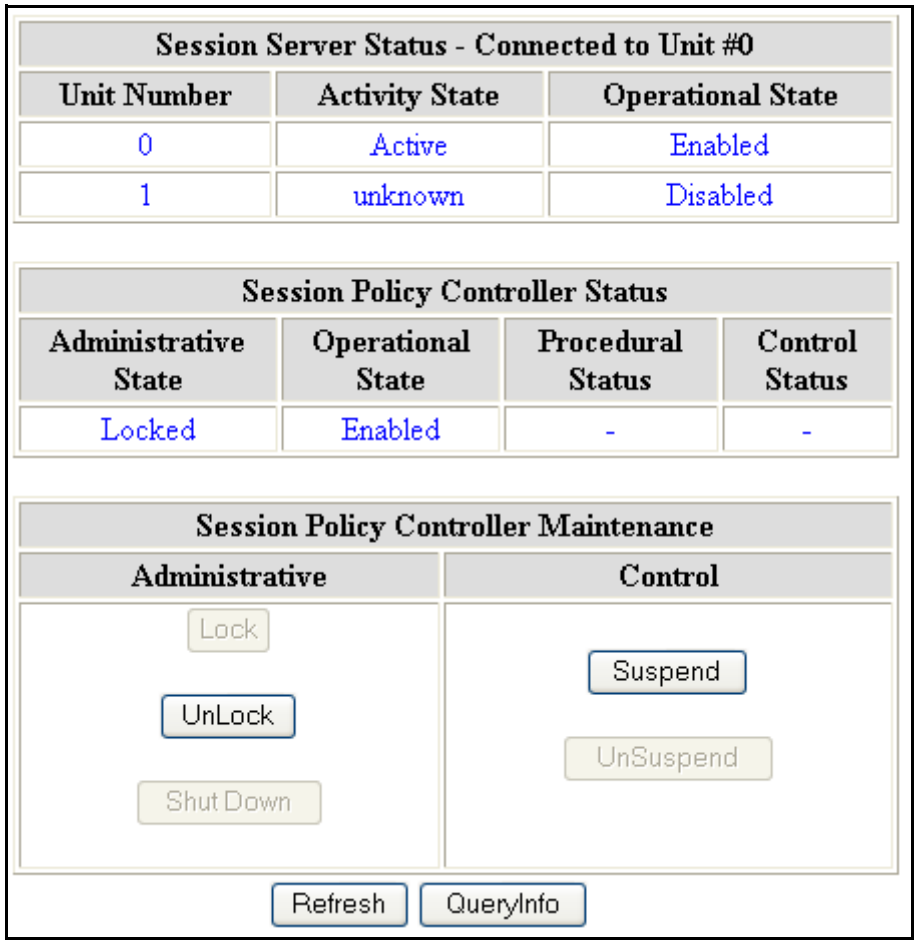


4 In the Policy Controller panel click **Unsuspend**.


Session Server Status - Connected to Unit #0
Unit Number
Activity State
Operational State
0
Active
Enabled
1
unknown
Disabled
Session Policy Controller Status
Administrative State
Operational State
Procedural Status
Control Status
Locked
Disabled
-
Suspended
Session Policy Controller Maintenance
Administrative
Control
Lock
UnLock
Shut Down
Suspend
UnSuspend
Refresh
QueryInfo

5 Monitor the status of the Policy Controller application in the Policy Controller Status box:

- the Operational State changes to **Enabled**
- the Control status changes to **-**



6 If necessary, bring the Policy Controller application back into service by executing procedure Unlock the Policy Controller application on page 145.

7 You have completed the procedure.

Prepare for a database restore on a Policy Controller unit

Purpose of this procedure

Use this procedure to prepare for a restoration of the Policy Controller application database from a backup copy.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of the high level upgrade activity Perform an emergency maintenance release rollback found in Upgrading the Policy Controller NTP, NN10431-461.

Limitations and Restrictions

CAUTION

Performing a restore of the Policy Controller application database is a service affecting activity and can cause data mismatches at the Communication Server 2000.

ATTENTION

For security reasons, you can only copy the database file from a remote server to the /users/mtc directory on the unit and you must use the secure copy command **scp** to perform this activity.

Automatic backup of the Policy Controller application database occurs at 1:00 AM each day on both Policy Controller units. This configuration setting cannot be modified and does not impact the use of this procedure.

The name of the backup database file is *solid.db.* Do not modify this name.

Prerequisites

You must have secure copy (scp) access to the Policy Controller unit from the remote system or other server location from where the database backup file solid.db is copied.

Action

From the remote server where the backup database file is located

1 Log onto the remote server, locate and navigate to the directory where the backup copy of the database file is stored.

2 Secure copy the database file to the Policy Controller unit you are restoring a backup copy of the database to by typing

```
$ scp solid.db mtc@<SS_IP_address>:
```

and pressing the Enter key.

where

SS_IP_address
is the IP address of the Policy Controller unit

The database file is copied to the /user/mtc directory on the target Policy Controller unit. This is the only Policy Controller directory that files can be copied into from an external server.

At a Policy Controller command line interface

3 Open a secure shell to the Policy Controller unit you are restoring a backup copy of the database to by typing

```
> ssh -l <userid> <SS_IP_address>
```

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

SS_IP_address
is the IP address of the Policy Controller

Example
ssh -l mtc 45.128.54.12

4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

5 When prompted, enter the root password.

6 Move the solid.db file you copied in step 2 from the /user/mtc directory to the /opt/apps/database/solid/backup directory by typing

$ mv /users/mtc/solid.db /opt/apps/database/solid/backup

and pressing the Enter key.

7 Change directory to the backup database directory by typing

$ cd/opt/apps/database/solid/backup

and pressing the Enter key.

8 Verify that the correct version (based on the file date) of the solid.db database file that you want to restore is located in the directory by typing

$ ls -l /opt/apps/database/solid/backup

and pressing the Enter key.

9 Verify that the presence of files *solid.ini* and *solmsg.out* files are also in the /opt/apps/database/solid/backup directory.

ATTENTION

The restorebackup.sh script does not run if you do not have the solid.ini and solmsg.out files located in the correct directory.

10 If the solid.ini file is not present, copy it into the backup directory by typing

$ cp /opt/apps/database/solid/dbfiles/solid.ini /opt/apps/database/solid/backup/solid.ini

and pressing the Enter key

11 If the solmsg.out file is not present, copy it into the backup directory by typing

$ cp /opt/apps/database/solid/dbfiles/solmsg.out /opt/apps/database/solid/backup/solmsg.out

and pressing the Enter key

12 Change the ownership of all files in the backup directory by typing

$ chown soliddb *

and pressing the Enter key.

13 Change the group of all files in the backup directory by typing

```
$ chgrp adm *
```

and pressing the Enter key.

14 Change the access permissions for all files in the backup directory by typing

```
$ chmod 600 *
```

and pressing the Enter key.

15 The database is now ready to be restored. You have completed this procedure. Return to the high-level activity.

Additional information

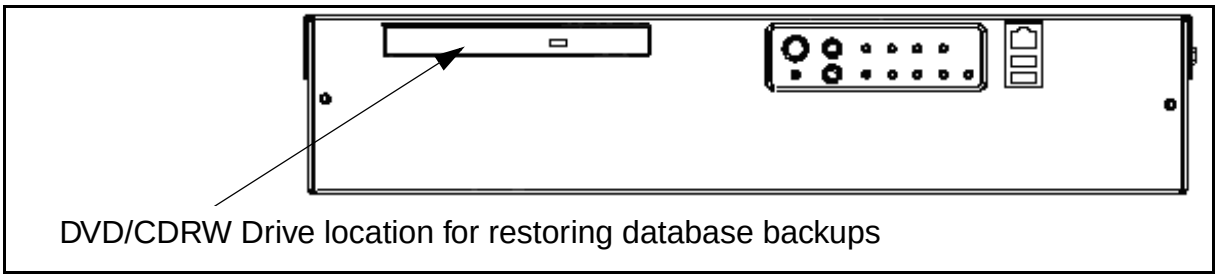
This section provides additional information regarding database restore activities.

To restore a backup database saved to a CD.

If you must restore a database backup that has been saved to a CD, you must first copy the database file from the CD to the default backup directory on the active Policy Controller unit. The selected backup database file must be restored to the following location:

/opt/apps/database/solid/backup/solid.db

To restore a backup of the database file to the backup directory, you must use a Policy Controller command line interface to copy the database file from a CD or CD-RW disk containing a copy of the back up database file to the opt/apps/database/solid/backup directory.



DVD/CDRW Drive location for restoring database backups

Ensure that you remove the CD disk from the DVD/CDRW drive, and store it in a safe place when you are done.

To restore a database backup save to another system

If you must restore a database backup that has been saved to another system, you must first copy the database file from the remote system back to the default backup directory on the active Policy Controller unit.

The selected backup database file must be restored to the following location:

/opt/apps/database/solid/backup

To restore a backup of the database to the backup directory you must use a Policy Controller command line interface to copy the database file solid.db from the remote system to the opt/apps/database/solid/backup directory. You may also be able to remote copy the backup database file from the remote system to the Policy Controller opt/apps/database/solid/backup directory. However, for security reasons, you may need to consult your site network administrator for instructions and permission to perform a remote copy.

Unlock the Policy Controller application

Purpose of this procedure

Use the following procedure to change the administrative status of the Policy Controller application to Unlocked, bringing the application into service.

Note: For more detailed information about Policy Controller application services states and administrative functions, refer to the Overview section of the Policy Controller Security and Administration NTP, NN10434-611.

Limitations and restrictions

This procedure provides instructions for changing the service status of the Policy Controller application software only. For instructions on determining the status of the Policy Controller platform, refer to procedure View the operational status of a Policy Controller NCGL platform on page 43

Prerequisites

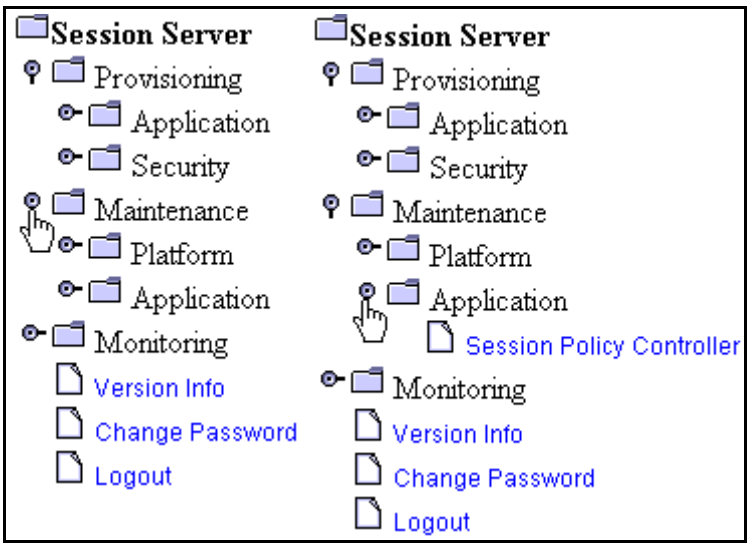
The active Policy Controller unit must be in a locked Administrative state. If it is not locked or you are uncertain of the state of the application, refer to procedure Lock the Policy Controller application on page 123.

Action

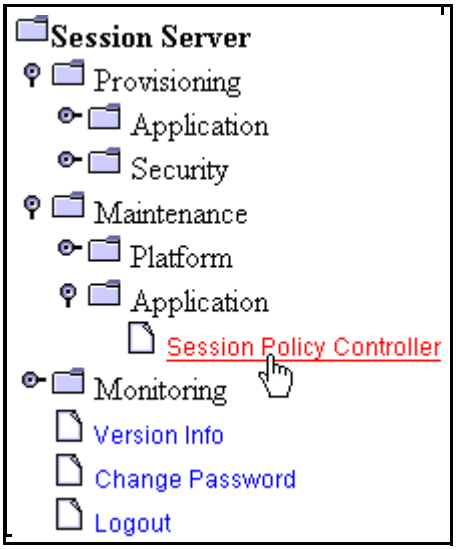
At the CS 2000 Session Server Launch Point

1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.

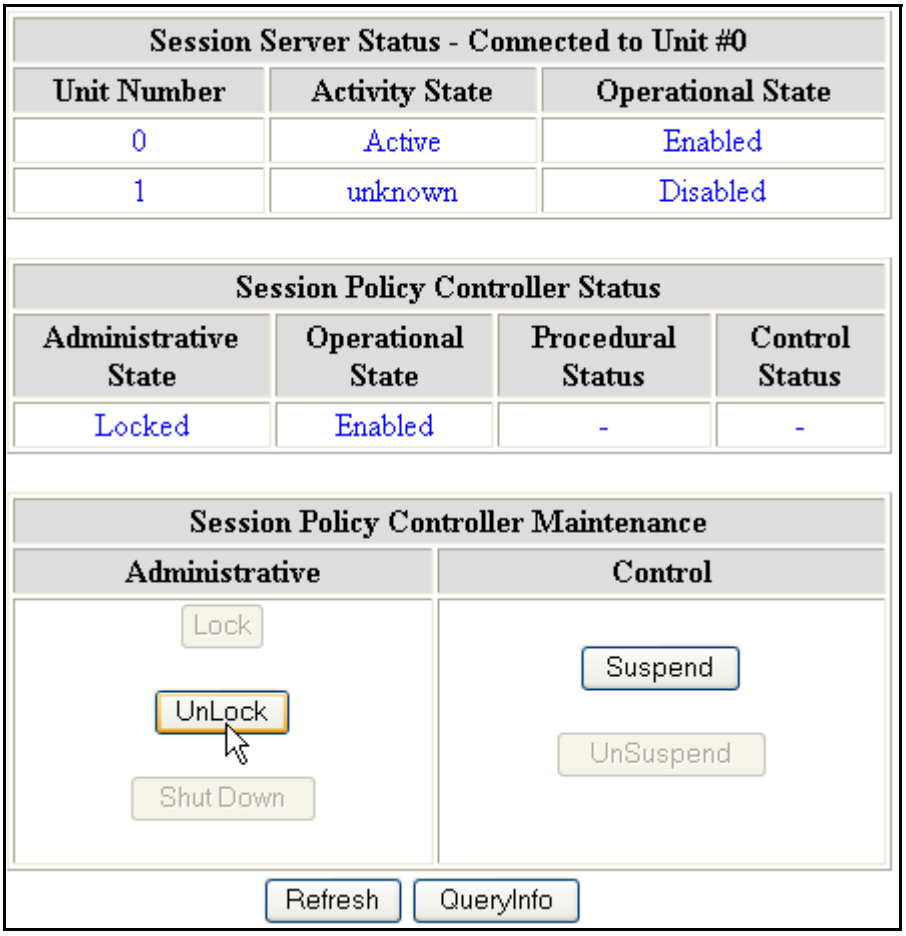
2 At the Session Server folder, click the **Maintenance folder,** then click the **Application** folder.



3 Click on the **Policy Controller** folder to open it.

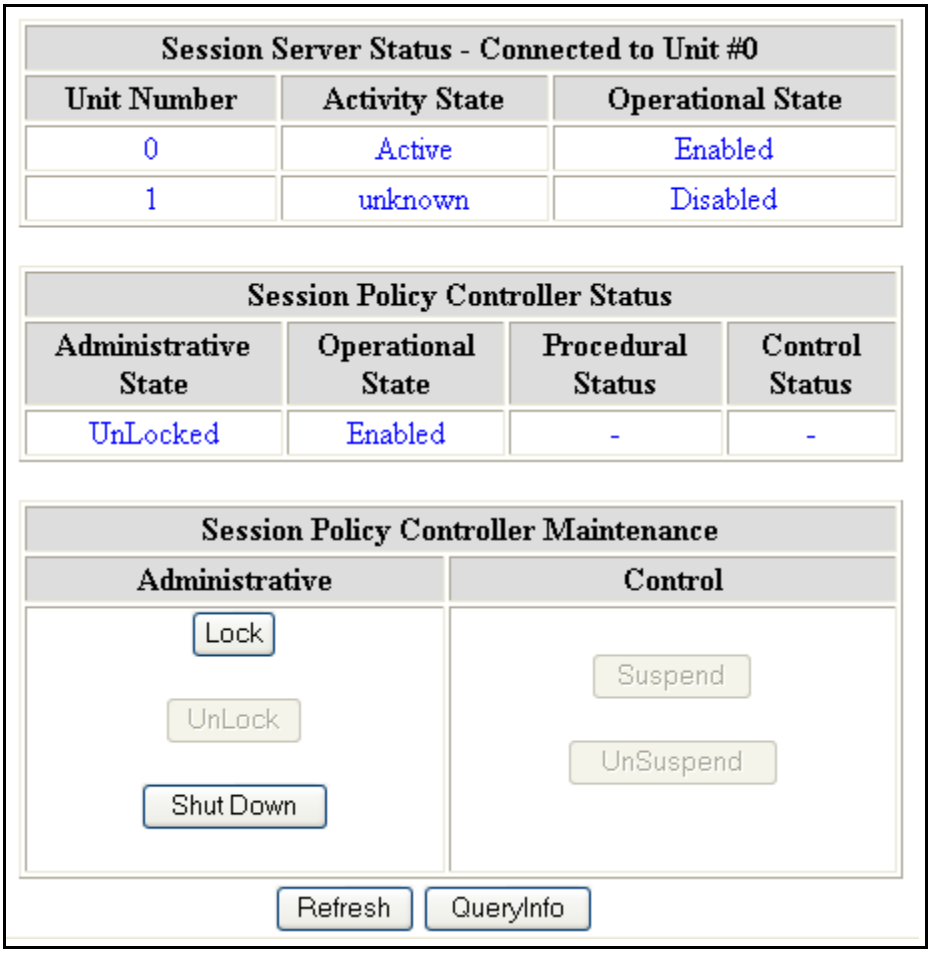


4 In the Policy Controller panel, click the **Unlock** button.

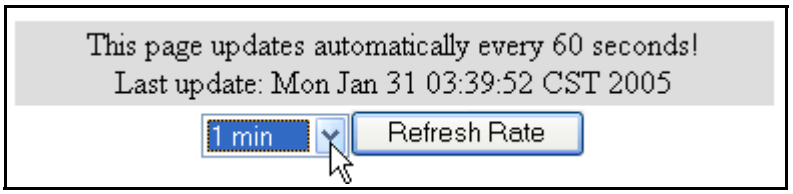

Session Server Status - Connected to Unit #0
Unit Number
Activity State
Operational State
0
Active
Enabled
1
unknown
Disabled
Session Policy Controller Status
Administrative State
Operational State
Procedural Status
Control Status
Locked
Enabled
-
-
Session Policy Controller Maintenance
Administrative
Control
Lock
UnLock
Shut Down
Suspend
UnSuspend
Refresh
QueryInfo

5 Monitor the status of the Policy Controller application in the Session Policy Controller Status box:

- the Administrative State changes to **Unlocked**



The status panel refreshes automatically according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the **Refresh Rate** button. Otherwise, manually refresh the panel by clicking on the **Refresh** button on the **Session Policy Controller Maintenance** panel.



6 You have completed this procedure.

Perform a manual backup of the Policy Controller database

Purpose of this procedure

Use this procedure to do the following tasks:

- Perform a backup of the Policy Controller application database of the active Policy Controller unit.
- Create regular backup copies of the database or as a precautionary activity before starting a maintenance release upgrade of the Policy Controller application.
- Perform as a standalone task or as part of a higher level upgrade activity

Limitations and Restrictions

CAUTION

If you perform provisioning changes during this procedure, it can lead to database corruption and possible system outages. To ensure that you create an accurate and complete copy of the active unit database, verify that all provisioning changes are stopped before continuing this procedure.

Prerequisites

ATTENTION

The Policy Controller database and the CS 2000 database must always be in sync. CS 2000 core images, CS 2000 GWC Manager Oracle database backups, and the Policy Controller application backups must always be maintained in sync for emergency recovery. To ensure they are in sync, perform images and backups at the same time.

Action

At a client workstation on the CS-LAN or IEMS client

1 Log into the active Policy Controller unit using a secure shell by typing

> **ssh -l <userid> <active_SS_IP_address>**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

active_SS_IP_address
is the IP address of the active Policy Controller

Example
ssh -l mtc 45.128.54.12

2 Change to the root user by typing

$ **su - root**

and pressing the Enter key.

3 When prompted, enter the root password.

4 Change to the database directory by typing

```
# cd /opt/apps/database/solid/dbfiles
```

and pressing the Enter key.

5 Put a copy of the database for the active unit in the backup directory by typing

```
# cp solid.db  /opt/apps/database/solid/backup
```

and pressing the Enter key.

Note: If other backup copies of the database exist with the same filename, you have the option of deleting those files or putting the backup copy into the backup directory under a new file name.

Example

```
# cp solid.db
/opt/apps/database/solid/backup/solid.db.backup1
```

6 For security purposes, ensure that you transfer a backup copy of the database file to a secure location.

Use the **scp** command to make a secure copy of the backup database file to a secure and remote server on your network. This server is contiguously available in case a restoration of the Policy Controller application database is necessary, such as during an upgrade rollback.

7 You have completed this procedure. Return to Step 3 in procedure Upgrade preparation on page 7.

Perform a database restore to a Policy Controller unit

Purpose of this procedure

Use this service impacting procedure to restore a Policy Controller application database from a backup copy to either the active or inactive Policy Controller units.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of the high level upgrade activity Perform an emergency maintenance release rollback found in the Upgrading the Policy Controller NTP, NN10431-461.

Limitations and Restrictions

CAUTION

Performing a restore of the Policy Controller application database is a service affecting activity and can cause data mismatches at the Communication Server 2000.

Prerequisites

You must first have completed procedure Prepare for a database restore on a Policy Controller unit on page 139.

Action

At a Session Server command line interface

1 Open a secure shell to the Policy Controller unit you are restoring a backup copy of the database to by typing

> **`ssh -l <userid> <SS_IP_address>`**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Policy Controller

SS_IP_address
is the IP address of either Policy Controller unit

Example
ssh -l mtc 45.128.54.12

2 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

3 When prompted, enter the root password.

4 Change directories by typing

```
$ /opt/apps/database/solid_install
```

and pressing the Enter key.

5 Run the database restore script by typing

```
$ ./restorebackup.sh
```

and pressing the Enter key.

6 You have completed this procedure. Return to the high-level activity.